Microsoft®
Training &
Certification

Microsoft Official
Curriculum

Module 10 : Résolution des problèmes d'accès réseau

Table des matières

Microsoft®

Notes du formateur

Présentation : 60 minutes

Atelier : 30 minutes

Ce module présente la résolution des problèmes d'accès réseau. Dans ce module, les stagiaires vont découvrir les procédures et les outils à utiliser pour dépanner une infrastructure réseau Microsoft® Windows Server™ 2003.

À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- identifier les ressources de résolution des problèmes d'accès réseau ;
- expliquer comment résoudre les problèmes d'authentification dans un réseau local (LAN, *Local Area Network*) ;
- expliquer comment résoudre les problèmes d'accès à distance.

Matériel requis

Pour animer ce module, vous devez disposer des éléments suivants :

- fichier Microsoft PowerPoint® file 2189A_10.ppt ;
- fichiers multimédias :
  - *Surveillance de l'accès à distance à l'aide de l'IAS*
  - *Tester une connexion sortante*

Important Il est recommandé d'utiliser PowerPoint 2002 ou une version ultérieure pour afficher les diapositives de ce cours. Si vous utilisez la visionneuse PowerPoint ou une version antérieure de PowerPoint, il est possible que certains éléments des diapositives ne s'affichent pas correctement.

Préparation

Pour préparer ce module, vous devez effectuer les tâches suivantes :

- lire tous les supports de cours de ce module ;
- vous exercer à effectuer les applications pratiques et l'atelier et vous reporter à la clé de réponse de l'atelier ;
- visualiser les présentations multimédias ;
- passer en revue les cours et modules de connaissances préalables.

Comment animer ce module

Ce module explique au stagiaire *comment* résoudre les problèmes, en supposant qu'ils maîtrisent déjà les procédures de base de résolution des problèmes. Ils doivent savoir lire un schéma simple de procédures. Ils doivent également savoir appliquer une procédure systématique pour identifier l'origine possible d'un problème et analyser les données pour déterminer la solution appropriée.

La résolution des problèmes étant un sujet complexe, il est impossible d'acquérir toutes les compétences en la matière dans un cours de cinq jours. Ce module contient des schémas Microsoft Visio® que les stagiaires peuvent utiliser comme support pour résoudre les problèmes d'accès à distance au réseau qui font appel à un grand nombre d'outils de résolution des problèmes.

Les stagiaires disposent de listes de ressources supplémentaires qu'ils peuvent utiliser pour obtenir des informations complémentaires sur les problèmes.

Pages d'instructions, applications pratiques et ateliers

Pages d'instructions

Les pages d'instructions contiennent des points de décision essentiels associés à la rubrique de la leçon. Vous allez utiliser ces instructions pour renforcer les acquis de la leçon et les objectifs.

Applications pratiques

Une fois que vous avez couvert le contenu de la section et montré les procédures de la leçon, expliquez aux stagiaires qu'une application pratique portant sur toutes les tâches abordées est prévue à l'issue de la leçon.

Ateliers

À la fin de chaque module, l'atelier permet aux stagiaires de mettre en pratique les tâches traitées et appliquées tout au long du module.

À l'aide de scénarios appropriés à la fonction professionnelle, l'atelier fournit aux stagiaires un ensemble d'instructions dans un tableau à deux colonnes. La colonne de gauche indique la tâche (par exemple : Créer un groupe). La colonne de droite contient des instructions spécifiques dont les stagiaires auront besoin pour effectuer la tâche (par exemple : À partir de **Utilisateurs et ordinateurs Active Directory**®, double-cliquez sur le nœud de domaine.).

Chaque exercice d'atelier dispose d'une clé de réponse que les stagiaires trouveront sur le CD-ROM du stagiaire s'ils ont besoin d'instructions étape par étape pour terminer l'atelier. Ils peuvent également consulter les applications pratiques et les pages de procédures du module.

Leçon : Ressources de résolution des problèmes d'accès réseau

Ce module explique le concept d'accès réseau et son rapport à la planification d'une infrastructure réseau Windows Server 2003. Dans ce module, le concept d'accès à distance n'est pas abordé d'un point de vue général, mais combine les connexions de réseau local (LAN), sans fil et d'accès à distance appelées accès réseau. Ce module porte sur la planification par les stagiaires de l'ensemble de leur stratégie d'accès réseau.

Journaux des accès réseau

Passez en revue les journaux figurant dans les pages et expliquez comment les stagiaires peuvent les utiliser pour résoudre les problèmes d'accès réseau. Dédiez un certain temps à l'étude des journaux qui ne sont pas familiers aux stagiaires.

Événements d'accès réseau

Expliquez aux stagiaires comment ils peuvent utiliser l'enregistrement des événements pour résoudre les problèmes d'accès réseau.

Outils d'analyse des accès réseau

Passez en revue les outils présentés dans cette rubrique. Si vous en avez le temps, présentez rapidement l'un des outils pour expliquer comment les stagiaires peuvent l'utiliser pour analyser les accès réseau.

Procédure associée aux ressources de résolution des problèmes de connexion LAN

Indiquez que la procédure des diapositives est incomplète. Les diapositives présentent un flux de procédures simple aux stagiaires qui ne sont pas familiers avec les opérations de résolution des problèmes. Passez en revue la procédure qui figure dans la page de la rubrique.

Procédure associée aux ressources de résolution des problèmes de connexion à distance

Indiquez que la procédure des diapositives est incomplète. Les diapositives présentent un flux de procédure simple aux stagiaires qui ne sont pas familiers avec les opérations de résolution des problèmes. Passez en revue la procédure qui figure dans la page de la rubrique.

Application pratique : Identification des ressources de résolution des problèmes d'accès réseau

Cette application pratique permet aux stagiaires d'évaluer leurs connaissances relatives à la sélection d'une méthode de connexion d'accès au réseau.

Leçon : Résolution des problèmes d'authentification LAN

Causes des erreurs d'authentification LAN

Passez en revue les principales causes des erreurs d'authentification LAN.

Enregistrement des événements de sécurité

Passez en revue les événements de l'audit des connexions aux comptes et les événements de l'audit des connexions.

Événements de l'audit de connexion aux comptes

Passez en revue les événements les plus courants qui figurent sur la page.

Audit des événements de connexion

Passez en revue les événements les plus courants qui figurent sur la page.

Instructions de résolution des problèmes d'accès LAN

Il s'agit d'instructions très importantes qu'il convient de décrire plus en détail.

Application pratique : Résolution des problèmes d'accès au réseau LAN

Cette application pratique permet aux stagiaires d'évaluer leurs connaissances relatives à la sélection d'une méthode de connexion d'accès au réseau.

Leçon : Résolution des problèmes d'accès à distance

Validation des certificats

Expliquez l'importance de la validation des certificats des utilisateurs et des ordinateurs.

Authentification à l'aide des journaux IAS

Passez en revue les problèmes les plus courants associés à la résolution des problèmes d'authentification.

Démonstration : Surveillance de l'accès à distance à l'aide de l'IAS

Passez en revue la démonstration pour vérifier que les stagiaires comprennent les principaux éléments présentés. Veillez à passer en revue la page multimédia avant de lancer la démonstration ; la page multimédia contient des questions essentielles dont les stagiaires doivent tenir compte pendant qu'ils regardent la démonstration.

Démonstration : Analyse des fichiers journaux d'authentification et de gestion des comptes IAS

Cette démonstration doit être dirigée par le formateur. Étudiez la démonstration avant de passer au cours en attachant une attention particulière aux éléments qui pourraient paraître confus pour les stagiaires.

Enregistrement PPP

Passez en revue les étapes associées à une connexion PPP (Point-to-Point Protocol) et les manières d'utiliser les journaux PPP pour résoudre les problèmes de connexion des clients.

Connexions d'accès à distance

Passez en revue chaque type de connexion et les actions que doivent exécuter les stagiaires pour résoudre les problèmes qui leur sont associés.

Authentification des accès sans fil

Expliquez comment le protocole MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol version 2) permet d'authentifier les utilisateurs, et passez en revue les outils à utiliser pour dépanner un point d'accès sans fil.

Problèmes VPN courants

Passez en revue les problèmes d'accès VPN (Virtual Private Network) et les stratégies à appliquer pour chacun d'entre eux.

Démonstration : Tester une connexion sortante

Passez en revue la démonstration pour vérifier que les stagiaires comprennent les principaux éléments présentés. Veillez à passer en revue la page multimédia avant de lancer la démonstration ; la page multimédia contient des questions essentielles dont les stagiaires doivent tenir compte pendant qu'ils regardent la démonstration.

Procédure de résolution des problèmes d'accès à distance au réseau

Passez en revue la procédure de résolution des problèmes d'accès à distance au réseau.

Instructions de résolution des problèmes d'accès à distance

Passez en revue les instructions et expliquez aux stagiaires pourquoi ils doivent tenir compte de chaque instruction. Vérifiez qu'ils comprennent les conséquences du non-respect de ces instructions.

Application pratique : Résolution des problèmes d'authentification des accès à distance

Cette application pratique permet aux stagiaires d'évaluer leurs connaissances relatives à la détermination d'un plan d'accès distant.

Atelier : Résolution des problèmes d'accès réseau

Informations générales sur l'atelier

L'atelier reflète l'approche appliquée au reste du module. Le scénario de l'exercice 1 expose un problème. Les stagiaires disposent des informations fournies par divers outils, qui leur permettent d'identifier le problème. Les stagiaires doivent analyser les informations fournies par divers outils de résolution des problèmes pour déterminer l'origine du problème. L'exercice 2 porte sur un autre scénario. Les stagiaires doivent déterminer une méthodologie et choisir les outils de résolution des problèmes qui fournissent les informations les plus pertinentes sur le problème.

Informations de personnalisation

Cette section identifie les caractéristiques des ateliers d'un module et les modifications apportées à la configuration des ordinateurs des stagiaires pendant les ateliers. Ces informations visent à vous aider à répliquer ou personnaliser le cours Microsoft Official Curriculum (MOC).

L'atelier de ce module dépend aussi de la configuration de la classe spécifiée dans la section Informations de personnalisation située à la fin du Guide de configuration automatisée de la classe du cours 2189*, Planification et maintenance d'une infrastructure réseau Microsoft Windows Server 2003*.

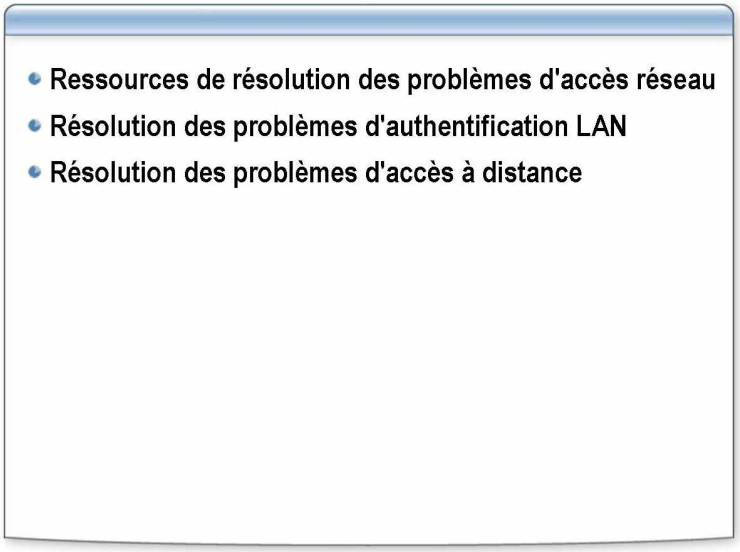
Mise en place de l'atelier

Aucune configuration de mise en place de l'atelier n'affecte la réplication ou la personnalisation.

Résultats de l'atelier

Aucun changement de configuration des ordinateurs des stagiaires n'affecte la réplication ou la personnalisation.

Vue d'ensemble



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

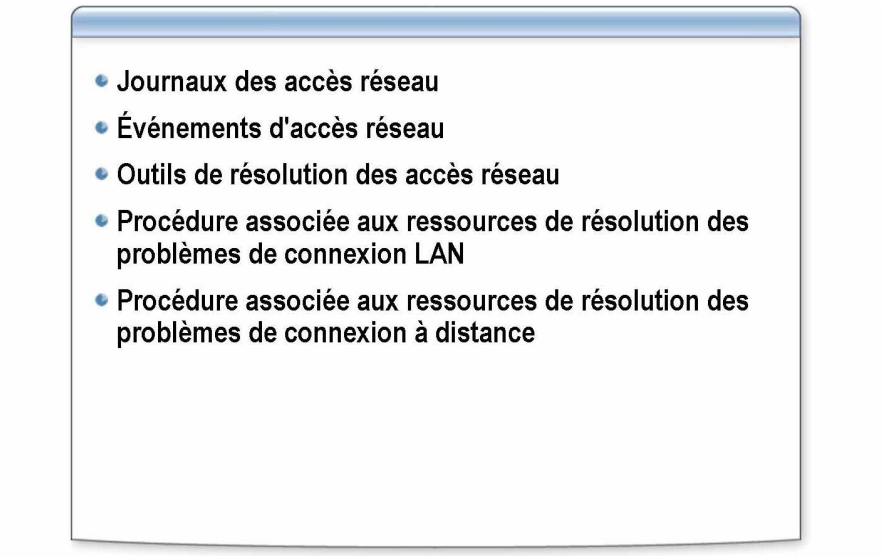
Ce module fournit des informations sur la résolution des problèmes d'accès réseau dans une infrastructure réseau Microsoft® Windows Server™ 2003. Il existe deux catégories principales d'accès réseau : LAN (Local Area Network) et accès à distance. Pour chacune des ces catégories, il existe des procédures et des outils qui permettent de résoudre les problèmes de connexion réseau.

Objectifs

À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- identifier les ressources de résolution des problèmes d'accès réseau ;
- expliquer comment résoudre les problèmes d'authentification LAN ;
- expliquer comment résoudre les problèmes d'accès à distance.

Leçon : Ressources de résolution des problèmes d'accès réseau



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Cette leçon porte sur les ressources de résolution des problèmes d'accès réseau. Elle identifie également les meilleures ressources disponibles pour résoudre les problèmes d'accès LAN et les problèmes d'accès à distance.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- identifier les journaux de résolution des problèmes d'accès réseau ;
- identifier les événements qui correspondent à des problèmes d'accès réseau ;
- identifier les outils de résolution des problèmes d'accès réseau ;
- expliquer la procédure associée aux ressources de résolution des problèmes de connexion LAN ;
- expliquer la procédure associée aux ressources de résolution des problèmes de connexion à distance.

Journaux des accès réseau

Journal	Utilisation
Journaux Authentification Windows ou Gestion des comptes Windows	Suivi de l'utilisation de l'accès réseau et des tentatives d'authentification ; particulièrement utile pour la résolution des problèmes de stratégies d'accès distant
Journaux PPP	Résolution des pannes de connexion PPP
Journaux IAS	Suivi de l'utilisation de l'accès réseau et des tentatives d'authentification
Enregistrement d'audit et Oakley	Surveillance des événements IPSec et résolution des échecs de connexion L2TP/IPSec
Journal de suivi IKE	Résolution des problèmes d'interopérabilité IKE dans certains cas

**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Vous pouvez utiliser différentes méthodes pour vous connecter à un réseau. La plupart de ces méthodes vous permettent de créer et d'analyser des journaux, des enregistrements de transactions ou d'activités, qui vous aident à résoudre les problèmes qui surviennent.

Journaux Authentification Windows ou Gestion des comptes Windows

Si vous utilisez un serveur, qui exécute la fonction Routage et accès distant de Windows Server 2003, comme serveur d'accès réseau, vous pouvez utiliser Authentification Windows® ou Gestion des comptes Windows. Lorsque l'une ou l'autre de ces fonctions est active, vous pouvez consigner dans des fichiers d'enregistrement locaux les informations d'authentification et de gestion des comptes Windows pour les connexions d'accès réseau. L'enregistrement est distinct de l'enregistrement des événements dans le journal système.

Les informations d'authentification et de gestion des comptes sont enregistrées dans un fichier journal configurable ou stockées dans le dossier *racinesystème*\System32\LogFiles (le dossier qui contient les fichiers système Windows 2003). Les fichiers journaux sont enregistrés dans un le format IAS (Internet Authentication Service) ou dans un format de base de données compatible, ce qui implique que n'importe quel programme de base de données peut lire le fichier journal directement pour l'analyser. Certains des journaux sont également stockés dans le format XML (Extensible Markup Language).

Vous pouvez utiliser les informations enregistrées dans les journaux d'authentification Windows et de gestion des comptes Windows pour identifier les accès réseau et les tentatives d'authentification. L'enregistrement des informations d'authentification et de gestion des comptes est très utile pour résoudre les problèmes associés aux stratégies d'accès distant. Pour chaque tentative d'authentification, le journal enregistre le nom et la stratégie d'accès distant qui a accepté ou rejeté la tentative de connexion.

Journaux PPP

L'enregistrement PPP (Point-to-Point Protocol) enregistre la série de fonctions de programmation et les messages de contrôle PPP au cours d'une connexion PPP. Il constitue une source d'information précieuse pour résoudre les problèmes associés à une connexion PPP défaillante. Par défaut, le journal PPP s'appelle ppp.log ; il est stocké dans le dossier *racinesystème*\Tracing.

Journaux IAS

Un serveur qui exécute Routage et accès distant prend en charge l'enregistrement des informations d'authentification et de gestion des comptes associées aux connexions d'accès réseau sur un serveur RADIUS (Remote Authentication Dial-In User Service) lorsque l'authentification et la gestion des comptes RADIUS sont actives. Cet enregistrement est distinct de l'enregistrement des événements dans le journal système. Lors de la configuration de l'enregistrement, vous pouvez définir :

- les demandes à enregistrer ;
- le format du fichier journal ;
- la fréquence de démarrage des nouveaux journaux ;
- la suppression automatique de l'ancien fichier journal lorsque le disque est saturé ;
- quand les fichiers journaux sont enregistrés ;
- le contenu des enregistrements des fichiers journaux.

Vous pouvez utiliser les informations enregistrées sur le serveur IAS pour identifier les accès réseau et les tentatives de connexion. Si le serveur RADIUS exécute IAS, les informations d'authentification et de gestion des comptes sont enregistrées dans des fichiers journaux stockés sur le serveur IAS. La procédure d'activation et de configuration de l'enregistrement est aussi simple que celle associée à un serveur qui exécute Routage et accès distant.

Vous pouvez utiliser la console IAS pour définir les demandes à enregistrer, le format du fichier journal, la fréquence de démarrage des nouveaux journaux et l'emplacement de stockage des fichiers journaux.

En outre, vous pouvez collecter ces informations dans un emplacement central et utiliser IAS pour créer des fichiers journaux en fonction des demandes d'authentification et de gestion des comptes qu'envoient les serveurs d'accès. Vous pouvez simplifier l'administration du service en configurant et en utilisant des fichiers journaux pour analyser les informations d'authentification telles que le rejet ou l'acceptation des connexions. Vous pouvez configurer et utiliser des journaux pour analyser les informations de gestion des comptes (telles que les enregistrements d'ouverture et de fermeture de sessions) et gérer les enregistrements à des fins de facturation.

Enregistrement d'audit et Oakley

Vous pouvez utiliser la fonction d'enregistrement d'audit de Windows Server 2003 pour contrôler les événements IPSec (Internet Protocol Security). Cette fonction constitue la méthode la plus rapide et la plus simple pour résoudre les problèmes de connexion L2TP (Layer Two Tunneling Protocol)/IPSec. Vous pouvez également activer le journal Oakley pour enregistrer toutes les négociations en mode principal ISAKMP (Internet Security Association and Key Management Protocol) ou en mode rapide.

Journal de suivi IKE

Certains scénarios IPSec peuvent nécessiter d'analyser plus précisément les négociations en mode principal IKE (Internet Key Exchange) et les négociations en mode rapide pour résoudre les problèmes. Vous pouvez activer le suivi des négociations IKE si les événements d'échec de l'audit ne fournissent pas suffisamment d'informations. Le journal de suivi IKE est un journal détaillé qui permet de résoudre les problèmes d'interopérabilité IKE dans certains cas. Vous devez maîtriser ISAKMP RFC 2408 et IKE RFC (Request For Comments) 2409 pour pouvoir interpréter les informations de ce journal.

Le journal de suivi IKE s'appelle *racinesystème*\Debug\Oakley.log. Il contient 50 000 lignes au maximum et les informations qu'il contient sont remplacées en fonction des besoins. Un nouveau fichier Oakley.log est créé chaque fois que le service IPSec démarre, la version précédente du fichier étant enregistrée sous le nom Oakley.log.sav. Lorsque le fichier est plein, le fichier est enregistré sous le nom Oakley.log.bak et un nouveau fichier Oakley.log est créé.

Du fait que de nombreuses négociations IKE ont lieu simultanément, vous devez réduire le nombre de négociations et activer l'enregistrement pendant une période aussi courte que possible pour disposer d'un journal plus clair et plus facile à interpréter.

Événements d'accès réseau

Journal des événements	Utilisation
Journal système	• Contient les informations émises par les divers services exécutés sur le système et enregistre les informations relatives à leur état • Enregistre les erreurs et les avertissements liés aux problèmes d'accès réseau
Journal sécurité	• Résout les échecs d'authentification Kerberos ou IPSec • Affiche les échecs de connexion lors de la tentative d'authentification d'un utilisateur

**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

L'enregistrement des événements correspond au stockage des événements dans divers journaux d'événements Windows Server 2003. En règle générale, vous enregistrez les événements pour résoudre des problèmes ou signaler aux administrateurs de réseau des événements inhabituels. Les journaux d'événements constituent une excellente source préliminaire pour analyser les problèmes d'accès réseau, car de nombreux services y enregistrent leurs erreurs et leurs avertissements.

Lorsque vous utilisez Stratégie de groupe pour activer l'audit des événements de connexion, vous pouvez appliquer la stratégie à l'unité d'organisation des contrôleurs de domaine pour que tous les contrôleurs de domaine enregistrent ces événements. Pour les événements de connexion de station de travail, vous pouvez définir la stratégie de groupe pour enregistrer les événements de connexion locaux.

Journaux système

Les journaux système contiennent des informations émises par les divers services exécutés sur le système et enregistrent des informations relatives à leur état. Des services, tels que l'accès distant et Net Logon, peuvent enregistrer des avertissements et des erreurs importants dans le journal système pour vous signaler des problèmes d'accès.

Vous pouvez activer l'enregistrement des événements et choisir le niveau de détail approprié dans la page **Propriétés** de l'onglet **Enregistrement** d'un serveur d'accès distant.

Le service Net Logon enregistre également, dans le journal système, les erreurs et les avertissements associés aux problèmes d'accès réseau. Si, par exemple, un problème de domaine autorisé empêche tous les utilisateurs d'un domaine de se connecter, le journal système contient un avertissement netlogon qui signale le problème.

Journaux de sécurité

L'enregistrement des événements de sécurité peut s'avérer d'une très grande utilité pour résoudre les problèmes d'authentification Kerberos ou IPSec. Lorsque ce type d'enregistrement est actif, vous pouvez identifier les problèmes de connexion lorsqu'un utilisateur tente de s'authentifier. Vous pouvez ainsi savoir ce qui s'est passé au cours de la procédure d'authentification et pourquoi la procédure a échoué.

Remarque Pour plus d'informations sur le protocole Kerberos, consultez l'article 217098 « Basic Overview of Kerberos User Authentication Protocol in Windows 2000 » (en anglais), à l'adresse http://support.microsoft.com/default.aspx?scid=kb;en-us;217098 dans la Base de connaissances de Microsoft.

Vous pouvez définir Stratégie de groupe pour auditer et comptabiliser les événements de connexion et collecter des informations sur l'authentification Kerberos.

Remarque Pour plus d'informations sur la résolution des problèmes Kerberos, consultez l'article 326985 « HOW TO:Troubleshoot Kerberos-Related Issues in IIS » (en anglais), à l'adresse http://support.microsoft.com/default.aspx?scid=kb;en-us;326985 dans la Base de connaissances de Microsoft.

Événements IPSec IKE

Les événements IPSec IKE (aboutissement et échec de la négociation) peuvent être également enregistrés dans le journal de sécurité.

Remarque Pour plus d'informations sur l'enregistrement des événements IPSec IKE, recherchez « DisableIKEAudits » dans les fichiers d'aide Windows Server 2003.

Lorsque vous activez l'audit du succès ou de l'échec de la stratégie d'audit **Auditer les événements de connexion**, IPSec enregistre les succès ou les échecs de chacune des négociations en mode principal ou en mode rapide ainsi que l'établissement et la fin de chaque négociation sous forme d'événements distincts. Toutefois, l'activation de ce type d'audit peut activer l'enregistrement des événements IKE dans le journal de sécurité. Par exemple, pour les serveurs connectés à Internet, les attaques sur le protocole IKE peuvent provoquer l'enregistrement d'événements IKE dans le journal de sécurité. Le journal de sécurité peut également contenir des événements IKE associés aux serveurs qui utilisent IPSec pour sécuriser le trafic vers de nombreux clients. Pour ne pas enregistrer les événements IKE dans le journal de sécurité, désactivez l'audit des événements IKE dans le journal en modifiant le paramètre de Registre **DisableIKEAudits**.

Attention Si vous ne modifiez pas correctement le Registre, vous risquez d'endommager gravement le système. Avant de modifier le Registre, sauvegardez toutes les données importantes de votre ordinateur.

Avertissement En règle générale, n'enregistrez pas en permanence les événements IPSec IKE, car ils peuvent générer d'importants volumes de données. Désactivez l'enregistrement après avoir résolu les problèmes.

Outils d'analyse des accès réseau

Outil	Utilisation
Diagnostic d'accès à distance	Collecte des journaux et informations détaillés relatifs à une connexion d'accès distant
Moniteur réseau	Recherche des réponses aux problèmes d'accès réseau et leurs solutions possibles
Netdom	Vérifie les serveurs et les approbations et réinitialise les approbations
Kerbtray	Permet de savoir si des tickets Kerberos ont été accordés dans le cache local
Moniteur de sécurité IP	Affiche les informations sur une stratégie IPSec active appliquée localement ou à un domaine, ainsi que les statistiques associées au processus d'échange de clés
Outils standard de résolution des problèmes réseau	Affiche la configuration IP des clients et le transfert de paquets

**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Vous pouvez utiliser divers outils en complément des journaux et des événements pour résoudre les problèmes d'accès réseau.

Diagnostic d'accès à distance

Vous pouvez utiliser les fonctions de diagnostic des accès distants de la famille Windows Server 2003 pour disposer de journaux détaillés sur les connexions d'accès à distance. Vous pouvez exécuter des diagnostics spécifiques en tapant la commande **netsh ras diag** sur la ligne de commandes.

Remarque Pour afficher la syntaxe de cette commande et les commandes disponibles, exécutez la commande **netsh ras diag** sur la ligne de commandes ou consultez les fichiers d'aide Windows Server 2003 pour plus d'informations.

Moniteur réseau

Moniteur réseau (ou tout autre analyseur de paquets) peut capturer le trafic réseau entre un client connecté et le serveur d'accès réseau. En analysant le trafic des accès réseau, vous pouvez analyser les problèmes d'accès et déterminer les solutions adaptées.

L'interprétation du trafic du réseau avec Moniteur réseau nécessite une connaissance approfondie des protocoles de communication. Vous pouvez enregistrer les fichiers capturés par Moniteur réseau et les envoyer à un expert en protocoles pour qu'il les analyse.

Netdom

Netdom (Network Domains) est un utilitaire de ligne de commandes qui permet à l'administrateur du réseau de vérifier les serveurs et les approbations, et de réinitialiser les approbations.

Kerbtray

Kerbtray est un utilitaire très pratique pour résoudre les problèmes Kerberos. L'utilitaire Kerbtray.exe est inclus dans le kit de ressources Microsoft Windows 2000. Kerbtray permet d'identifier les tickets Kerberos accordés dans le cache local. Vous pouvez télécharger cet utilitaire à l'adresse http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/kerbtray-o.asp (en anglais).

Remarque Pour plus d'informations sur l'utilitaire Kerbtray et des conseils pour résoudre les problèmes Kerberos, consultez l'article « Authentication for Administrative Authority » (en anglais) à l'adresse http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/authent.asp.

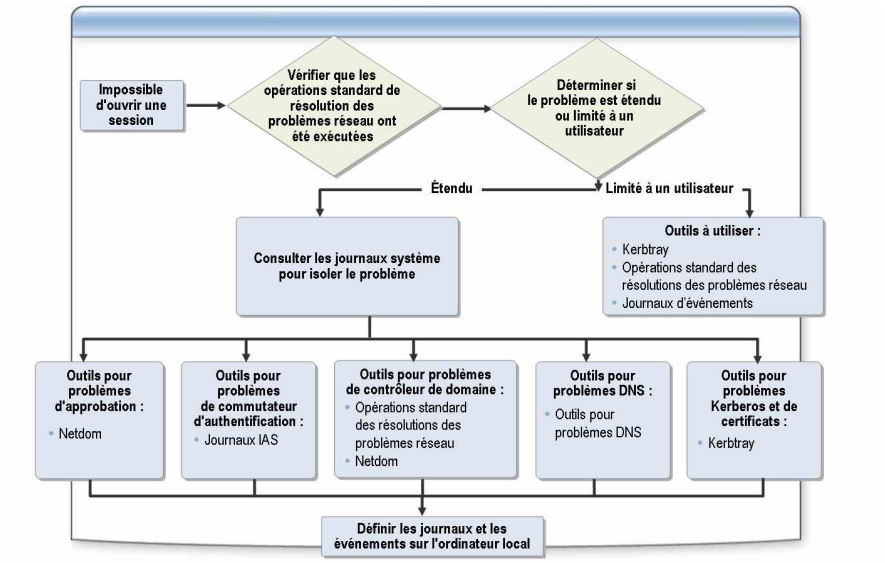
Moniteur de sécurité IP

Le Moniteur de sécurité IP (Internet Protocol) est un outil qui permet d'effectuer des opérations avancées de résolution des problèmes IPSec. Il permet d'obtenir des informations sur une stratégie IPSec active appliquée localement ou à un domaine, en complément des statistiques associées au processus d'échange de clés.

Utilitaires standard de résolution des problèmes réseau

Outre les utilitaires d'accès réseau, vous pouvez également utiliser des outils standard de résolution des problèmes spécifiques tels que ipconfig, ping, pathping, traceroute, etc.

Procédure associée aux ressources de résolution des problèmes de connexion LAN



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Comme pour toute activité de dépannage, vous devez disposer d'une procédure que vous devez appliquer pour résoudre les problèmes d'accès réseau. Une fois la procédure définie, vous devez définir les ressources à utiliser pour identifier et résoudre les problèmes de connexion LAN.

Procédure

Il est important de vous souvenir que vous devez toujours collecter en premier lieu des informations générales, puis des informations plus spécifiques au fur et à mesure des besoins pour résoudre un problème. Bien souvent, vous pouvez résoudre les problèmes en analysant les informations des journaux d'événements, qui sont plus aisées à collecter et qui ont un caractère plus général. Après avoir déterminé qu'un utilisateur ne peut pas se connecter, vous devez suivre les étapes suivantes pour résoudre les problèmes de connexion LAN :

- vérifier que les opérations standard de résolution des problèmes ont été exécutées ;
- déterminer si le problème touche plusieurs utilisateurs ou s'il est limité à un seul utilisateur ;
- afficher les journaux systèmes appropriés ;
- Si les journaux système ne contiennent pas suffisamment d'informations, collectez d'autres informations en utilisant les journaux et les événements de l'ordinateur local ;
- Une fois le problème identifié, utilisez les outils appropriés pour le résoudre.

Journaux de l'Observateur d'événements

Consultez toujours les journaux de l'Observateur d'événements en premier pour y rechercher des informations sur la tentative de connexion. Si vous avez activé l'audit des événements de connexion et des événements de connexion aux comptes, vous pouvez collecter des informations pertinentes en cas de problèmes associés à Kerberos. Ces informations peuvent également vous aider à identifier les problèmes associés à IPSec.

Kerbtray

Si nécessaire, collectez des informations plus détaillées sur le problème. Si, par exemple, le problème est lié à Kerberos, vous avez besoin d'informations complémentaires que vous pouvez obtenir avec l'utilitaire Kerbtray pour résoudre le problème.

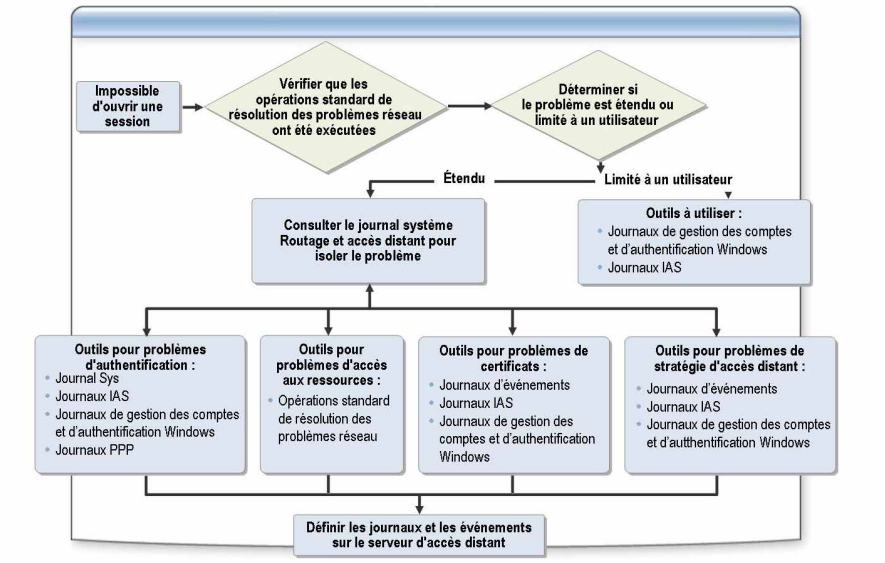
Journaux RADIUS

Si l'authentification RADIUS est utilisée avec la connexion, vous pouvez utiliser les journaux RADIUS. Ces journaux peuvent contenir des informations importantes sur le problème.

Moniteur réseau

Si vous ne parvenez pas à déterminer le problème en utilisant d'autres méthodes, identifiez l'interaction du protocole lui-même que vous pouvez analyser en utilisant Moniteur réseau ou un autre analyseur de protocole. Toutefois, ces informations ne sont utiles que si vous maîtrisez le protocole concerné. Si tel n'est pas le cas, vous devez faire appel à un expert en la matière.

Procédure associée aux ressources de résolution des problèmes de connexion à distance



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Après avoir défini la procédure de résolution des problèmes de connexion à distance, vous devez sélectionner les ressources à utiliser pour résoudre les problèmes.

Procédure

La procédure de résolution des problèmes de connexion à distance est similaire à celle des connexions LAN, mais la différence principale réside dans le fait que le problème est vraisemblablement lié à l'ordinateur client. Après avoir déterminé qu'un utilisateur ne peut pas se connecter, vous devez suivre les étapes suivantes pour résoudre les problèmes de connexion à distance :

- vérifier que les opérations standard de résolution des problèmes réseau ont été exécutées ;
- déterminer si le problème concerne plusieurs utilisateurs ou s'il est limité à un seul utilisateur ;
- consulter les journaux système Routage et accès distant pour identifier le problème ;
- si les journaux système ne contiennent pas suffisamment d'informations, collectez des informations complémentaires en utilisant les journaux et les événements de l'ordinateur local ;
- une fois le problème identifié, utilisez les outils appropriés pour le résoudre.

Journal des événements

Si vous utilisez un serveur qui exécute Routage et accès distant comme serveur d'accès réseau et que l'enregistrement des événements est actif, le journal des événements peut contenir des informations pertinentes qui peuvent vous aider à résoudre le problème d'accès à distance. Certains problèmes peuvent être résolus immédiatement et d'autres peuvent nécessiter des informations plus complètes.

Journaux de gestion des comptes et d'authentification Windows

Si vous utilisez un serveur, qui exécute Routage et accès distant, comme serveur d'accès réseau, vous pouvez également collecter plus d'informations dans les journaux de gestion des comptes et d'authentification Windows ou les journaux de gestion des comptes et d'authentification RADIUS.

Netsh

L'utilitaire de ligne de commandes Netsh, qui permet d'effectuer des diagnostics sur les accès distants, peut également s'avérer utile à ce stade si vous avez besoin d'informations complémentaires.

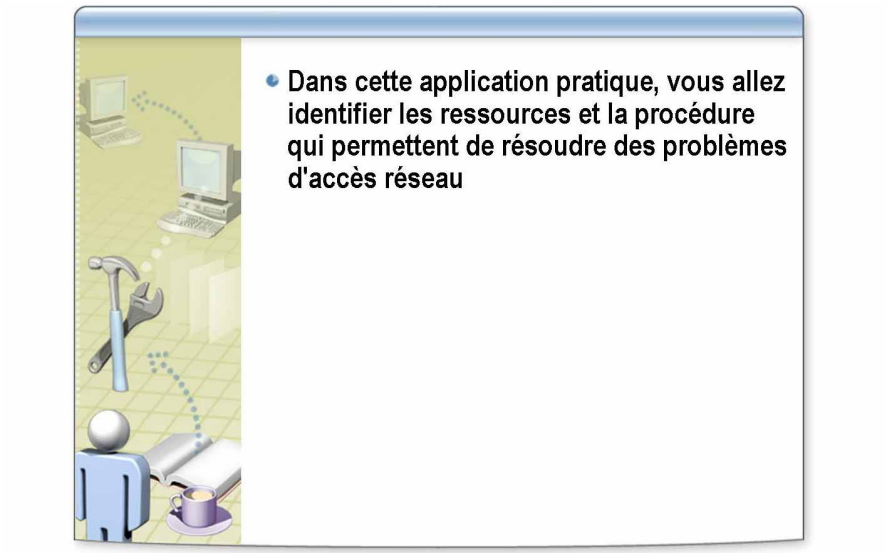
Autres journaux

Vous pouvez collecter des informations détaillées supplémentaires dans des journaux configurables tels que les journaux PPP ou le journal Oakley pour résoudre les problèmes associés à L2TP/IPSec.

Moniteur réseau

Si vous ne parvenez pas à identifier le problème en utilisant d'autres méthodes, vous devez l'analyser au niveau des protocoles que vous devez maîtriser pour pouvoir résoudre le problème. Moniteur réseau permet de capturer les informations nécessaires à l'analyse des protocoles.

Application pratique : Identification des ressources de résolution des problèmes d'accès réseau



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Dans cette application pratique, vous allez identifier les ressources et la procédure qui permettent de résoudre des problèmes d'accès réseau.

Objectif

L'objectif de cette application pratique vise à identifier les ressources de résolution des problèmes d'accès réseau.

Instructions

1. Lisez le scénario.
2. Préparez-vous à discuter des difficultés associées à cette tâche après l'application pratique.

Scénario

Vous êtes employé comme consultant par Contoso, Ltd, un fournisseur de solutions de connexion réseau. Du fait du développement rapide de la société, la charge de travail des techniciens de l'assistance réseau a augmenté et la société doit embaucher des techniciens de premier niveau pour répondre aux besoins d'assistance. Actuellement, la société résout les problèmes de connexion en collectant et en analysant les données des journaux de suivi appropriés et les captures de paquets. Toutefois, les nouveaux employés ne disposent pas des connaissances nécessaires pour interpréter ces données et nécessitent d'autres méthodes pour faciliter les opérations de résolution des problèmes.

Application pratique

Quels autres outils et méthodes recommandez-vous pour le personnel d'assistance pour faciliter la résolution des problèmes d'accès réseau ?

Au lieu de commencer par utiliser les informations très détaillées des fichiers de suivi et des captures de paquets, le personnel de l'assistance technique doit apprendre à collecter et interpréter les informations des journaux d'événements et des journaux de gestion des comptes et d'authentification du serveur qui exécute Routage et accès distant ou du serveur IAS, selon le fournisseur d'authentification qui a été configuré.

Si les informations de ces journaux ne permettent pas de trouver une solution, vous pouvez collecter des informations plus précises dans des journaux et les partager avec les ingénieurs logiciels de la société ou les experts spécialisés dans les protocoles d'accès réseau.

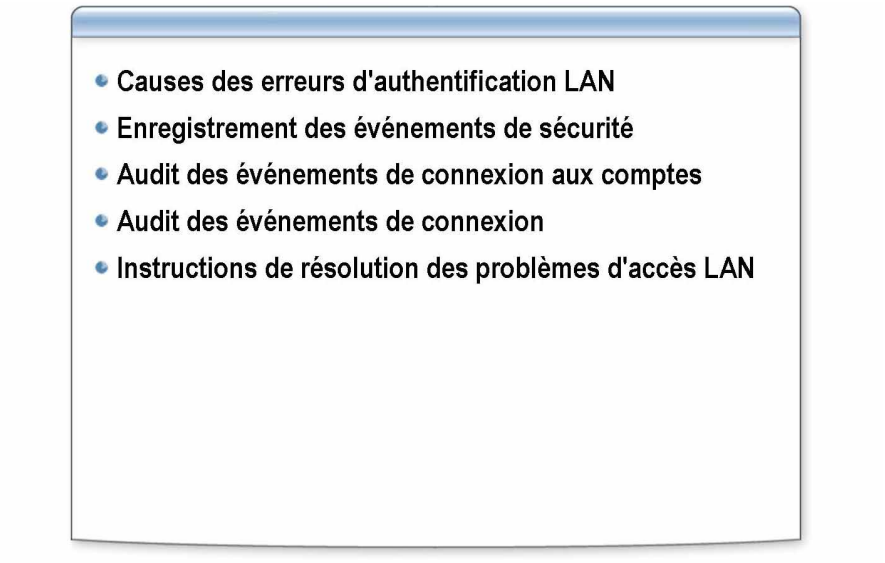
_____

_____

_____

_____

Leçon : Résolution des problèmes d'authentification LAN



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

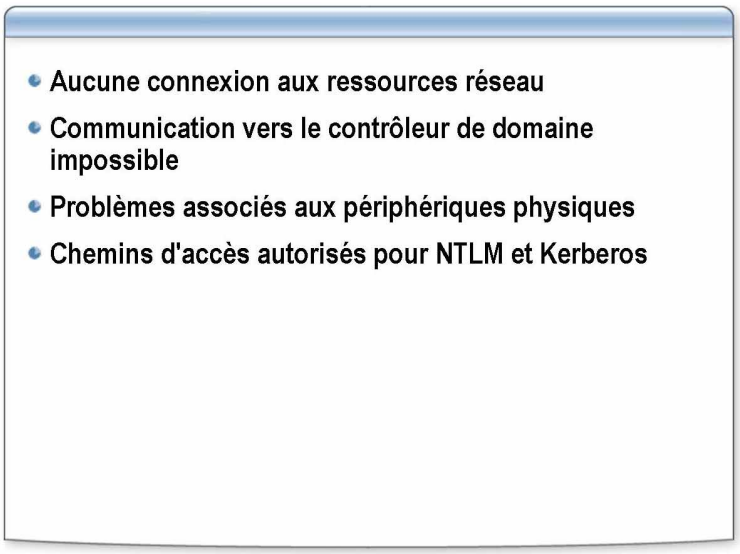
Cette leçon porte sur la résolution des problèmes d'authentification LAN. Les problèmes d'authentification LAN peuvent avoir plusieurs origines. Cette leçon identifie les problèmes les plus courants ainsi que les outils que vous pouvez utiliser pour les résoudre.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- identifier l'origine des erreurs d'authentification LAN ;
- expliquer comment utiliser les journaux d'audit pour résoudre les problèmes d'authentification ;
- identifier les événements de connexion aux comptes de l'audit ;
- identifier les événements de connexion de l'audit ;
- appliquer les instructions de résolution des problèmes d'accès LAN.

Causes des erreurs d'authentification LAN



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Les problèmes d'authentification LAN les plus courants sont liés à l'approbation des chemins d'accès et à l'impossibilité de communiquer avec un contrôleur de domaine.

Aucune connexion aux ressources réseau

L'impossibilité de s'authentifier sur le LAN peut être liée à l'impossibilité de se connecter à d'autres ressources réseau telles qu'un serveur DHCP (Dynamic Host Configuration Protocol), un serveur DNS (Domain Name System), etc. La connectivité de base à ces ressources doit exister pour que l'authentification puisse avoir lieu.

Communication vers le contrôleur de domaine impossible

Vous pouvez être à même de vous connecter au réseau, d'obtenir une adresse IP et même de résoudre le nom d'un contrôleur de domaine, mais, selon le protocole d'authentification utilisé, vous devez communiquer à un moment donné avec un contrôleur de domaine. Si vous ne pouvez pas communiquer avec le contrôleur de domaine, la procédure d'authentification échoue.

Problèmes associés aux périphériques physiques

S'il existe des problèmes associés aux périphériques physiques, vous ne pouvez pas vous connecter en appliquant cette méthode. Vous devez utiliser la procédure standard de résolution des problèmes pour garantir la connectivité entre les clients, les ressources du réseau et les contrôleurs du domaine.

Description d'un chemin d'accès autorisé

Un *chemin d'accès autorisé* est défini par une série de liens autorisés entre deux domaines qui se transmettent les demandes d'authentification. Le chemin d'accès autorisé est implémenté par le service Net Logon via un appel de procédure distante authentifiée (RPC, *Remote Procedure Call*) vers l'autorité de domaine autorisée, à savoir le contrôleur du domaine.

Chemins d'accès autorisés pour NTLM et Kerberos

S'il existe une référence à la demande d'authentification, un chemin est calculé pour l'authentification directe NTLM (NT Lan Manager) ou une référence Kerberos en utilisant les informations relatives à l'arborescence et aux raccourcis de relations d'approbation pour déterminer le chemin d'accès au domaine de destination.

Remarque Pour plus d'informations sur les chemins autorisés pour NTLM et Kerberos, consultez le document à l'adresse suivante : http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/maintain/kerberos.asp (en anglais).

Dans le calcul du chemin d'accès, les raccourcis de relations d'approbation permettent de contourner les domaines supérieurs de la hiérarchie. Les raccourcis de relations d'approbation qui peuvent exister dans chaque niveau de l'arborescence sont vérifiés. S'il en existe une vers le domaine de destination, le domaine suivant de l'arborescence n'est pas vérifié.

- NTLM

  Lorsque vous utilisez le protocole NTLM, le serveur doit contacter un service d'authentification de domaine sur un contrôleur de domaine pour vérifier les informations d'identification du client. Un serveur authentifie un client en envoyant ces informations à un contrôleur du domaine du compte du client.

- Kerberos

  Lorsque vous utilisez le protocole Kerberos, le serveur ne contacte pas le contrôleur de domaine. Le client obtient un ticket d'un serveur en en demandant un à un contrôleur du domaine du compte du serveur et le serveur valide le ticket sans consulter une autre autorité.

Problèmes courants

Le tableau suivant répertorie les problèmes courants associés aux connexions LAN. Ces erreurs et d'autres erreurs figurent dans le journal système.

Numéro d'erreur	Description	Conseils de résolution des problèmes
Erreur 0x6	Nom du client introuvable (nom principal inconnu).	Lorsque cette erreur se produit, vérifiez si le nom figure dans le service d'annuaire Active Directory®. S'il s'y trouve, vérifiez si le compte a expiré. Il peut arriver qu'un utilisateur soit au milieu d'une session et que son compte soit soudainement verrouillé.
Erreur 0x7	Le nom du serveur est introuvable (nom principal inconnu).	Lorsque cette erreur se produit, vérifiez si le nom figure dans Active Directory. S'il s'y trouve, vérifiez si le compte a expiré. Il peut arriver qu'un utilisateur soit au milieu d'une session et que son compte soit soudainement verrouillé.
Erreur 0x17	Le mot de passe a expiré ; changer le mot de passe pour résoudre le problème.	Si un ticket d'accord de ticket est dans le cache et que le mot de passe de l'utilisateur a expiré ou qu'il a été modifié, cela implique qu'il existe un conflit au niveau des informations d'identification. L'utilisateur doit se déconnecter, puis se reconnecter pour que les informations d'identification correspondent.
Erreur 0x1F	Échec de la vérification de l'intégrité du champ décrypté.	Il est vraisemblable que le client n'a pas reçu l'adresse exacte du serveur qu'il recherche. Vous devez commencer par rechercher le problème au niveau du service DNS ou du service utilisé pour la résolution des noms.

(*suite*)

Numéro d'erreur	Description	Conseils de résolution des problèmes
Erreur 0x29	Flux de messages modifié.	Il est vraisemblable que le client n'a pas reçu l'adresse exacte du serveur qu'il recherche. Vous devez commencer par rechercher le problème au niveau du service DNS ou du service utilisé pour la résolution des noms.
Erreur 0x20	Le ticket a expiré.	Plus la valeur du paramètre « Durée de vie maximale du ticket utilisateur » est petite, plus cette erreur se produit.
Erreur 0x25	Demande de session répétée.	Cette erreur indique qu'un authentificateur est apparu deux fois. Il se peut qu'un intrus essaie de réexécuter une session ou simplement qu'une carte réseau soit défaillante.
Erreur 0x25	Le décalage d'horloge est trop important.	Bien que cette erreur soit présente dans les journaux, elle n'empêche pas l'utilisateur d'être authentifié. Si les informations d'identification de l'utilisateur sont valides, l'utilisateur est identifié lors de la seconde tentative.

Enregistrement des événements de sécurité

Catégorie d'audit	Description
Audit des événements de connexion aux comptes	Déterminez si vous voulez auditer chaque connexion ou déconnexion d'un utilisateur avec un autre ordinateur pour lequel le contrôleur de domaine valide le compte Générés lorsqu'un compte d'utilisateur de domaine est authentifié sur un contrôleur de domaine. L'événement est enregistré dans le journal de sécurité du contrôleur du domaine
Audit des événements de connexion	Déterminez si vous voulez auditer chaque connexion ou déconnexion d'un utilisateur avec un ordinateur local Générés lorsqu'un utilisateur local est authentifié sur un ordinateur local. L'événement est enregistré dans le journal de sécurité local

**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

L'enregistrement des événements de sécurité peut s'avérer très utile pour résoudre les problèmes d'authentification Kerberos et NTLM. Lorsque cette fonction est active, vous pouvez identifier les échecs de connexion lorsque les utilisateurs tentent de s'authentifier. Ces informations doivent vous permettre de mieux comprendre les événements qui se produisent au cours de la procédure de l'authentification et d'identifier l'origine de l'erreur.

Deux catégories d'audit Stratégie de groupe sont particulièrement utiles pour résoudre les problèmes d'authentification LAN : l'audit des événements de connexion aux comptes et l'audit des événements de connexion.

Définition du paramètre de stratégie

La définition du paramètre de stratégie permet d'indiquer si vous voulez auditer les succès ou les échecs ou ne pas auditer du tout ce type d'événement. L'audit des succès génère une entrée d'audit lorsqu'une tentative de connexion à un compte aboutit. L'audit des échecs génère une entrée d'audit lorsqu'une tentative de connexion au compte échoue.

Vous pouvez définir cette valeur dans la boîte de dialogue **Propriétés** du paramètre de cette stratégie. Vous devez activer la case à cocher **Définir ces paramètres de stratégie** et désactiver les cases à cocher **Réussite** et **Échec**. La valeur par défaut est Réussite.

Si l'audit des succès des événements de connexion aux comptes est actif sur un contrôleur de domaine, une entrée est enregistrée pour chaque utilisateur qui est validé par rapport au contrôleur de domaine, même si l'utilisateur est connecté à une station de travail qui est jointe au domaine.

Audit des événements de connexion aux comptes

Le paramètre de sécurité Auditer les événements de connexion aux comptes permet d'indiquer si vous voulez auditer les connexions d'un utilisateur à un autre ordinateur et chacune des déconnexions de l'utilisateur de l'ordinateur pour lequel le contrôleur de domaine valide le compte. Des événements de connexion à un compte sont générés lorsqu'un compte d'utilisateur de domaine est authentifié sur un contrôleur de domaine. L'événement est enregistré dans le journal de sécurité du contrôleur du domaine.

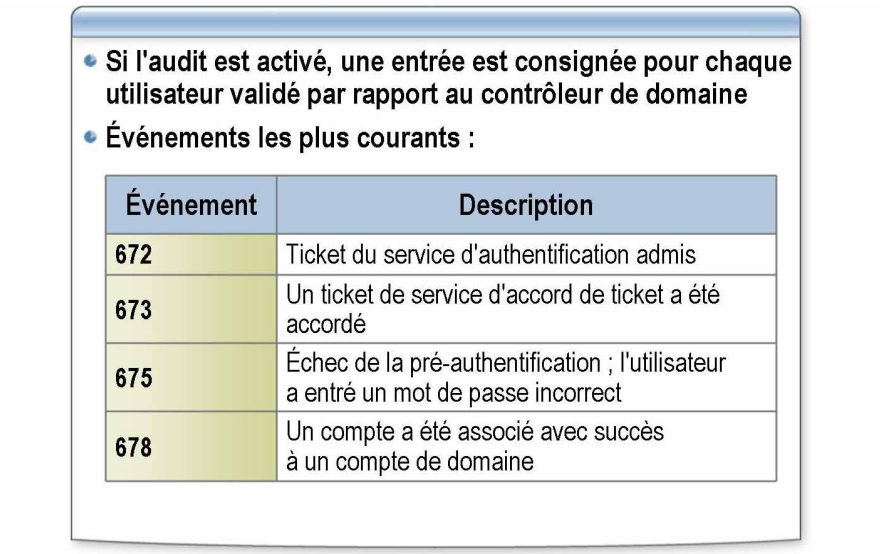
Si vous définissez ce paramètre de stratégie, vous pouvez indiquer si vous voulez auditer les succès ou les échecs ou ne pas auditer du tout ce type d'événement. L'audit des succès génère une entrée d'audit lorsqu'une tentative de connexion à un compte aboutit. L'audit des échecs génère une entrée d'audit lorsqu'une tentative de connexion au compte échoue.

Audit des événements de connexion

Ce paramètre de sécurité permet d'indiquer si vous voulez auditer les connexions d'un utilisateur à un autre ordinateur ou les déconnexions de cet ordinateur. Des événements de connexion sont générés lorsqu'un utilisateur local est authentifié sur un ordinateur local. L'événement est enregistré dans le journal de sécurité local.

Si vous définissez ce paramètre de stratégie, vous pouvez indiquer si vous voulez auditer les succès ou les échecs ou ne pas auditer du tout ce type d'événement. L'audit des succès génère une entrée d'audit lorsqu'une tentative de connexion à un compte aboutit. L'audit des échecs génère une entrée d'audit lorsqu'une tentative d'ouverture de session échoue.

Audit des événements de connexion aux comptes



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Lors de l'analyse d'un événement de connexion à un compte, vous découvrez les événements qui décrivent le problème de sécurité qui existe.

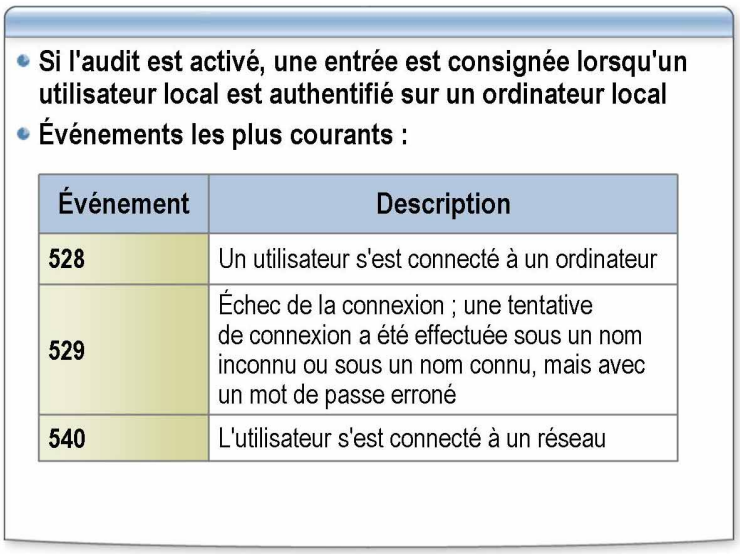
Audit des événements de connexion aux comptes

Le tableau suivant répertorie les ID des événements accompagnés de leur description.

ID d'événement	Description
672	Un ticket AS (Autonomous Systems) d'un service d'authentification a été émis et validé.
673	Un ticket de service de génération de ticket (TGS) a été accordé.
674	Une entité de sécurité a renouvelé un ticket AS ou un ticket TGS.
675	Échec de la procédure de pré-authentification. Cet événement est généré dans un centre de distribution de clés (KDC, *Key Distribution Center*) lorsqu'un utilisateur tape un mot de passe erroné.
678	Un compte a été associé avec succès à un compte de domaine.
682	Un utilisateur s'est reconnecté à une session Terminal Server déconnectée.
683	Un utilisateur s'est déconnecté d'une session Terminal Server sans fermer la session.

Remarque Pour plus d'informations sur chacun des ID d'événements, consultez l'article 326985 « HOW TO: Troubleshoot Kerberos-Related Issues in IIS » (en anglais), à l'adresse http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b326985, dans la Base de connaissances de Microsoft.

Audit des événements de connexion



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Le paramètre de sécurité Auditer les événements de connexion permet d'indiquer si vous voulez auditer les connexions et les déconnexions d'un utilisateur à ou depuis un ordinateur.

Événements courants de connexion aux comptes

Le tableau suivant répertorie les ID des événements accompagnés de leur description. Les événements les plus courants sont les événements 528, 529 et 540.

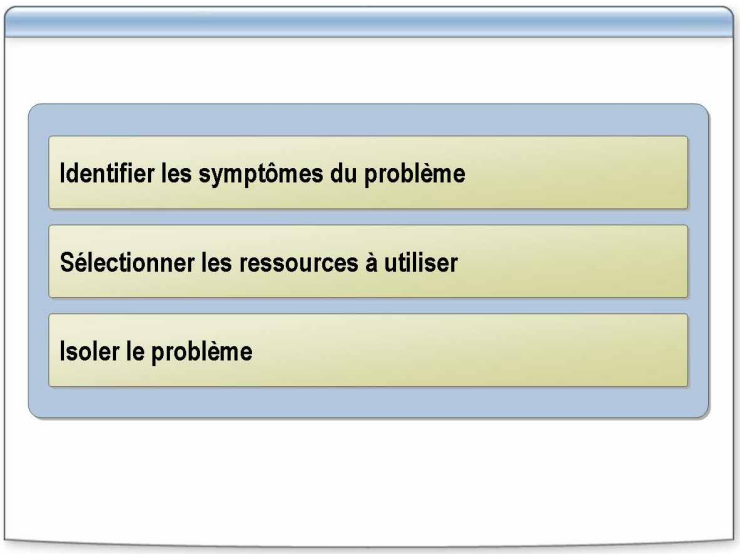
ID d'événement	Description
528	Un utilisateur s'est connecté à un ordinateur.
529	Échec de la connexion. Une tentative de connexion a été effectuée sous un nom inconnu ou sous un nom connu, mais avec un mot de passe erroné.
530	Échec de la connexion. Une tentative de connexion a été effectuée par un utilisateur en dehors du délai autorisé.
531	Échec de la connexion. Une tentative a été effectuée à l'aide d'un compte désactivé.
532	Échec de la connexion. Une tentative de connexion a été effectuée à l'aide d'un compte qui a expiré.
533	Échec de la connexion. Un utilisateur a tenté de se connecter à un ordinateur auquel il n'est pas autorisé à accéder.
534	Échec de la connexion. L'utilisateur a tenté de se connecter en utilisant un type non autorisé.
535	Échec de la connexion. Le mot de passe du compte défini a expiré.
536	Échec de la connexion. Le service Net Logon n'est pas actif.
537	Échec de la connexion. La tentative de connexion a échoué pour d'autres raisons. **Remarque :** dans certains cas, l'origine de l'échec peut rester inconnue.

(*suite*)

ID d'événement	Description
538	L'utilisateur a exécuté la procédure de déconnexion.
539	Échec de la connexion. Le compte était verrouillé lorsque la tentative de connexion a eu lieu.
540	L'utilisateur s'est connecté à un réseau.
541	La procédure d'authentification IKE en mode principal a été exécutée entre l'ordinateur local et l'homologue listé (en établissant une association de sécurité) ou bien le mode rapide a établi un canal de données.
542	Un canal de données a été arrêté.
543	Le mode principal a été arrêté. **Remarque :** cette fin peut se produire à la suite de l'expiration de l'association de sécurité (le délai par défaut est de huit heures), de la modification de la stratégie ou du fait de l'homologue.
544	L'authentification en mode principal a échoué parce que l'homologue n'a pas fourni un certificat valide ou que la signature n'a pas été validée.
545	L'authentification en mode principal a échoué à la suite d'une erreur Kerberos ou parce que le mot de passe est erroné.
546	L'établissement de l'association de sécurité IKE a échoué parque que l'homologue a envoyé une demande non valide. Un paquet contenant des données non valides a été reçu.
547	Une erreur s'est produite lors d'une négociation IKE.
548	Échec de la connexion. L'identificateur de sécurité (SID, *Security ID*) du domaine autorisé ne correspond pas à celui du domaine du compte de l'utilisateur.
549	Échec de la connexion. Tous les SID qui correspondent à des espaces de noms non autorisées ont été filtrés lors de l'authentification dans les forêts.
550	Message de notification qui peut indiquer une tentative d'attaque de refus de service.
551	L'utilisateur a lancé la procédure de déconnexion.
552	L'utilisateur s'est connecté à un ordinateur en utilisant des informations d'identification explicites alors qu'il était déjà connecté sous un autre nom d'utilisateur.
682	L'utilisateur s'est reconnecté à une session Terminal Server déconnectée.
683	L'utilisateur s'est déconnecté d'une session Terminal Server sans fermer la session. **Remarque :** cet événement est généré lorsque l'utilisateur est connecté à une session Terminal Server dans le réseau. Il apparaît sur le serveur terminal.

Remarque Pour plus d'informations sur les événements les plus courants, consultez l'article 326985 « HOW TO: Troubleshoot Kerberos-Related Issues with IIS » (en anglais), à l'adresse http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b326985 dans la Base de connaissances de Microsoft.

Instructions de résolution des problèmes d'accès LAN



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

La résolution des problèmes d'accès LAN peut s'avérer très pénible. Vous devez définir une procédure et identifier les outils appropriés. Les instructions suivantes vont vous permettre de déterminer la meilleure méthodologie de résolution des problèmes pour votre entreprise.

Appliquez la procédure suivante pour résoudre les problèmes d'accès LAN :

- Identifiez les symptômes du problème

  Vous devez vérifier les symptômes du problème du client. Vous devez également vérifier les ressources du réseau pour vous assurer qu'il ne s'agit pas d'un problème matériel

- Sélectionnez les ressources à utiliser

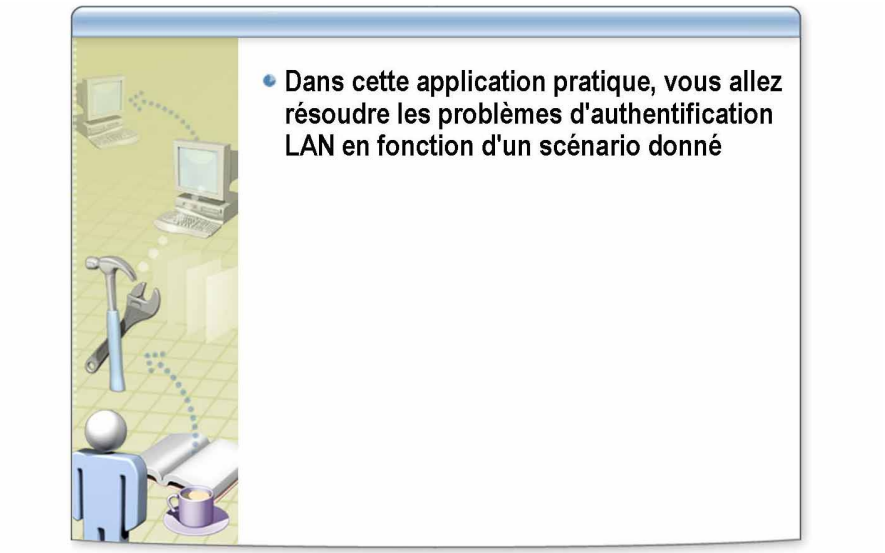
  Sélectionnez les ressources appropriées en fonction des symptômes du problème. Après avoir sélectionné les ressources, vous devez activer l'audit des événements de connexion et l'audit des événements de connexion aux comptes.

- Isolez le problème

  Après avoir sélectionné les ressources, vous devez déterminer la meilleure méthode d'utilisation des ressources pour isoler le problème.

Conseil Pour disposer d'un outil permanent de résolution des problèmes, vous pouvez acheter ou créer une application qui contrôle des événements particuliers du journal d'événements et vous signale leur déclenchement.

Application pratique : Résolution des problèmes d'accès au réseau LAN



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Dans cette application pratique, vous allez identifier la procédure de résolution des problèmes d'authentification LAN.

Objectif

L'objectif de cette application pratique vise à résoudre un problème d'authentification LAN.

Instructions

1. Lisez le scénario.
2. Préparez-vous à discuter des difficultés associées à cette tâche après l'application pratique.

Scénario

Vous êtes ingénieur système chez Contoso, Ltd, une grande société qui a déployé Windows Server 2003 Active Directory avec trois domaines. Le siège de la société se trouve à Zürich, en Suisse, et dispose de trois filiales principales aux États-Unis.

L'administrateur système de la société San Diego, en Californie, vous signale qu'un utilisateur ne peut pas se connecter au domaine Recherche. Il est tôt à San Diego et la plupart des employés n'est pas encore arrivée au travail.

Application pratique

Quel plan appliquez-vous pour résoudre le problème ?

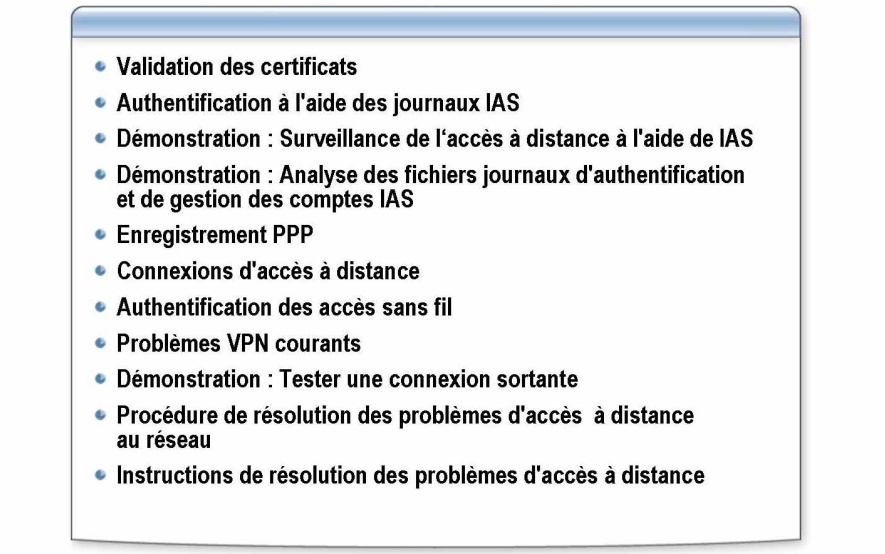
Tout d'abord, vérifiez si l'administrateur système a déterminé si le problème affecte uniquement l'utilisateur ou s'il touche d'autres utilisateurs.

S'il n'affecte que l'utilisateur, concentrez vos actions sur la station de travail. Analysez le journal système pour y rechercher des informations pertinentes et appliquez les procédures standard de résolution des problèmes réseau, si nécessaire.

Si le problème affecte d'autres utilisateurs, vérifiez les journaux système des contrôleurs du domaine Recherche. Recherchez les derniers événements et erreurs, notamment ceux de Netlogon. Vérifiez les journaux du serveur DNS pour déterminer s'ils contiennent des problèmes d'enregistrement qui peuvent empêcher de déterminer l'emplacement des contrôleurs du domaine. Vous devez également analyser les erreurs ou les avertissements émis par le protocole Kerberos ou IPSec ou le service LSASrv. LSASrv est le service associé à l'autorité de sécurité locale (LSA, *Local Security Authority*). LSA est le sous-système de sécurité qui est responsable de tous les services d'authentification et d'autorisation interactives d'un ordinateur local. LSA est également utilisé pour traiter les demandes d'authentification via le protocole Kerberos v5 ou le protocole NTLM dans Active Directory.

Selon le problème que vous identifiez, vous devez appliquer d'autres techniques de résolution des problèmes. L'activation de l'audit des événements de connexion et de l'audit des événements de connexion aux comptes peut vous aider à collecter des informations supplémentaires.

Leçon : Résolution des problèmes d'accès à distance



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

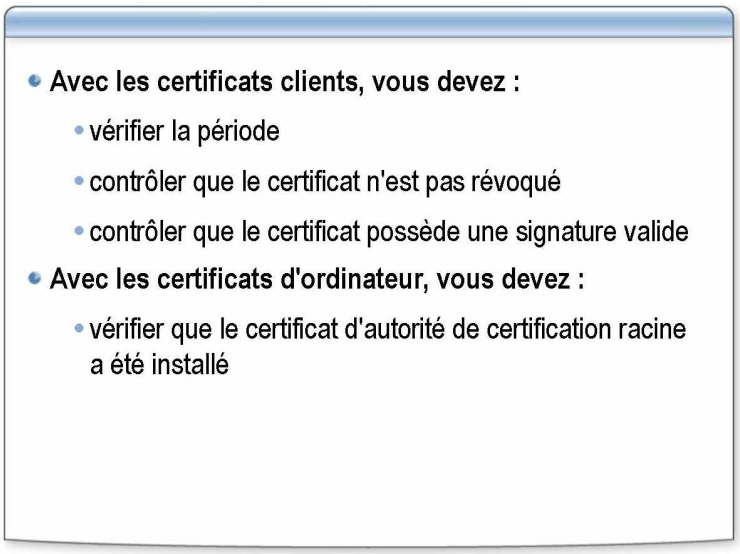
Lorsque vous travaillez avec un système d'accès à distance, la plupart des problèmes que vous rencontrez sont liés à des composants que vous ne contrôlez pas. Apprendre à identifier précisément la source d'un problème d'accès à distance est très utile. Cette leçon contient des informations sur la résolution des problèmes d'accès à distance à un réseau.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- expliquer comment résoudre les problèmes de validation des certificats ;
- expliquer comment résoudre les problèmes d'authentification en utilisant les journaux IAS ;
- expliquer comment surveiller les accès distants à l'aide de IAS ;
- expliquer comment analyser les fichiers journaux d'authentification et de gestion des comptes IAS ;
- expliquer comment résoudre les problèmes de connexion en utilisant les journaux PPP ;
- expliquer comment résoudre les problèmes de connexion d'accès à distance ;
- expliquer comment résoudre les problèmes d'accès sans fil ;
- expliquer comment résoudre les problèmes de connexion VPN (Virtual Private Network) courants ;
- expliquer la procédure de résolution des problèmes d'accès à distance au réseau ;
- appliquer les instructions de résolution des problèmes d'accès à distance.

Validation des certificats



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Au cours d'une procédure d'authentification qui utilise un certificat, il est nécessaire de valider le certificat de l'utilisateur et celui de l'ordinateur. Des erreurs peuvent se produire à l'un ou l'autre bout de la procédure de validation.

Procédure des certificats

Lorsque le protocole EAP-TLS (Extensible Authentication Protocol–Transport Level Security) est utilisé pour l'authentification, le client qui accède au réseau envoie un certificat d'utilisateur et le serveur d'authentification (le serveur d'accès distant ou le serveur RADIUS) envoie un certificat d'ordinateur.

Les certificats peuvent être également utilisés pour l'authentification au cours de la phase de négociation L2TP/IPSec IKE. Dans ce cas, le client et le serveur d'accès distant doivent disposer de certificats valides. Les certificats sont utilisés de deux manières différentes. La première validation de certificat se produit lorsque vous vous connectez. Une fois le certificat validé, le tunnel est configuré et connecté. Une fois que vous êtes connecté, l'authentification PPP a lieu.

Erreurs de certificat

Le tableau suivant répertorie les erreurs les plus courantes associées aux clients qui accèdent au réseau, qui se produisent lorsque les utilisateurs ne peuvent pas s'authentifier en utilisant des certificats. Ces erreurs et d'autres erreurs sont enregistrées dans le journal système.

Erreur	Description	Origine de l'erreur
766	Une connexion qui utilise le protocole L2TP sur IPSec nécessite d'installer un certificat de machine appelé certificat d'ordinateur.	En règle générale, cette erreur est générée sur un serveur d'accès distant ayant des ports actifs L2TP configurés. Le service d'accès distant a démarré, mais aucun certificat n'est enregistré dans le magasin des certificats de l'ordinateur.
781	La connexion nécessite un certificat pour effectuer un appel L2TP.	Cette erreur se produit lorsque la connexion nécessite un certificat et qu'aucun certificat valide ne se trouve sur le client lors de l'appel L2TP.

Certificats clients valides

Si vous utilisez la méthode d'authentification EAP-TLS, il doit exister un certificat client valide sur une carte à puce ou dans le magasin de certificats local. Pour que l'authentification fonctionne correctement, vérifiez que chaque certificat de la chaîne de certificats envoyés par le client répond aux conditions suivantes :

- La date en cours doit se trouver dans les dates de validité du certificat.

  Les certificats ne peuvent être utilisés que pendant une période donnée.

- Le certificat ne doit pas avoir été révoqué.

  Les certificats émis peuvent être révoqués à tout moment.

- Le certificat doit avoir une signature numérique valide.

  Les autorités de certification signent numériquement les certificats qu'elles émettent. Le serveur IAS vérifie la signature numérique de chaque certificat de la chaîne, à l'exception de celle du certificat CA (Certificate Authority) racine, en obtenant la clé publique de l'autorité de certification du certificat et en validant mathématiquement la signature numérique.

Utilisation avancée de la clé

Le certificat client doit contenir également le rôle du certificat d'authentification du client (appelé également Utilisation avancée de la clé) ayant l'identificateur d'objet 1.3.6.1.5.5.7.3.2 ainsi qu'un nom d'utilisateur principal de compte d'utilisateur valide ou un nom de domaine complet de compte d'ordinateur valide pour la propriété Autre nom de l'objet du certificat.

Certificat d'ordinateur valide

Le serveur d'authentification doit disposer, dans son magasin Autorités de certification racines de confiance, du certificat CA racine de l'autorité de certification du certificat du client d'accès à distance pour valider la chaîne de certificats du client d'accès à distance.

En outre, le serveur d'authentification vérifie que l'identité envoyée dans le message EAP-Response/Identity correspond au nom figurant dans la propriété Autre nom de l'objet du certificat. Cette opération empêche un utilisateur mal intentionné d'usurper l'identité d'un utilisateur définie dans le message EAP-Response/Identity.

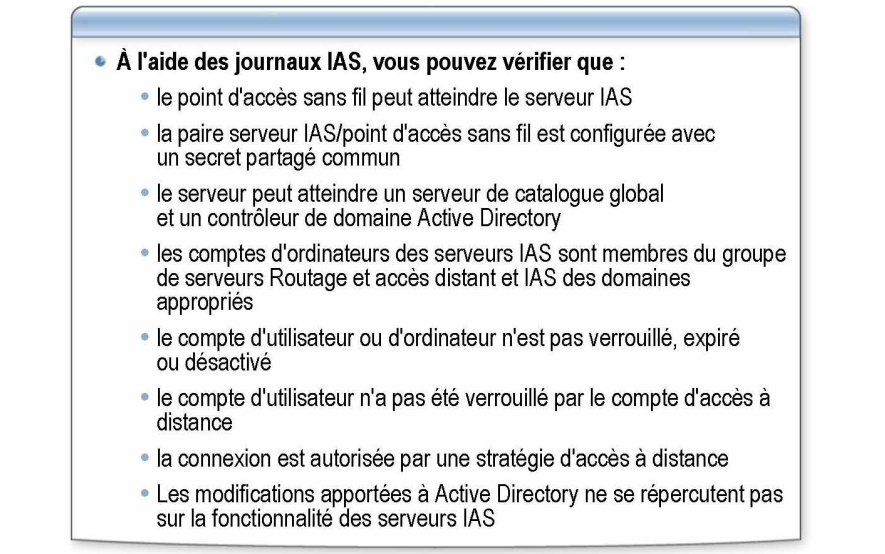
Paramètres de Registre IAS

Si le serveur d'authentification est un serveur IAS, les paramètres de Registre suivants de la clé **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\13** peuvent modifier le comportement de EAP-TLS lors de la révocation des certificats.

Comportement EAP-TLS	Description	Paramètres
IgnoreNoRevocationCheck	Vous pouvez utiliser cette entrée pour authentifier les clients lorsque le certificat ne contient pas de points de distribution de la liste de révocation de certificats, tels que ceux des tiers.	1 = Activé 0 = Désactivé (valeur par défaut)
IgnoreRevocationOffline	IAS ne permet pas aux clients de se connecter s'il ne peut pas vérifier que l'un des certificats de leur chaîne de certificats a été révoqué. Lorsqu'il ne peut pas se connecter à un serveur contenant une liste de révocation de certificats, EAP-TLS considère que la procédure de vérification de révocation du certificat a échoué.	1 = Permet aux clients EAP-TLS de se connecter et empêche les échecs de validation provoquer par des dysfonctionnements réseau 0 = Hors ligne (valeur par défaut)
NoRevocationCheck	La procédure de vérification de révocation détermine si le certificat du client d'accès à distance et les certificats de sa chaîne de certificats n'ont pas été révoqués. **NoRevocationCheck** est affecté de la valeur 0 par défaut.	1 = Empêche EAP-TLS de vérifier le certificat. 0 = Désactivé (valeur par défaut)
NoRootRevocationCheck	Cette entrée élimine uniquement la vérification de révocation du certificat CA racine du client. Une vérification de révocation est toujours exécutée sur les autres certificats de la chaîne du client d'accès à distance.	1 = IAS empêche EAP-TLS d'effectuer une vérification de révocation sur la racine du client d'accès à distance 0 = Désactivé (valeur par défaut)

Tous ces paramètres de Registre doivent être ajoutés avec le type DWORD et doivent être affectés de la valeur 0 ou 1. Le client d'accès à distance n'utilise pas ces paramètres.

Authentification à l'aide des journaux IAS



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Si vous utilisez un serveur IAS, les problèmes d'authentification sont enregistrés dans les journaux IAS. Il se peut que vous deviez résoudre des problèmes liés aux protocoles d'authentification CHAP (Challenge Handshake Authorization), EAP (Extensible Authentication Protocol) etc. Vous pouvez utiliser les journaux IAS pour déterminer l'existence d'un problème d'authentification.

Résolution des problèmes courants

Si vous utilisez IAS comme solution d'authentification, vous devez vérifier les éléments suivants pour résoudre les problèmes courants :

- Les points d'accès sans fil doivent pouvoir atteindre les serveurs IAS

  Pour vérifier ces éléments, essayez de taper l'adresse IP du port non contrôlé du point d'accès sans fil sur les serveurs IAS. En outre, vérifiez que les stratégies IPSec, les filtres de paquets IP et les autres mécanismes qui limitent le trafic réseau n'empêchent pas l'échange de messages RADIUS (ports UDP [User Datagram Protocol] 1812 et 1813) entre le point d'accès et ses serveurs IAS configurés.
- Chaque paire serveur IAS/point d'accès sans fil doit être configurée avec un secret partagé commun.
- Les serveurs doivent pouvoir atteindre un serveur de catalogue global et un contrôleur de domaine Active Directory.
- Les comptes d'ordinateurs des serveurs IAS doivent être membres du groupe de serveurs de routage et d'accès distant et IAS des domaines appropriés.
- Le compte d'utilisateur ou d'ordinateur ne doit pas être verrouillé, ne doit pas avoir expiré ou ne doit pas être désactivé ou l'heure de connexion doit correspondre à la page d'heures autorisées.
- Le compte d'utilisateur ne doit pas avoir été verrouillé par le verrouillage du compte d'accès à distance.

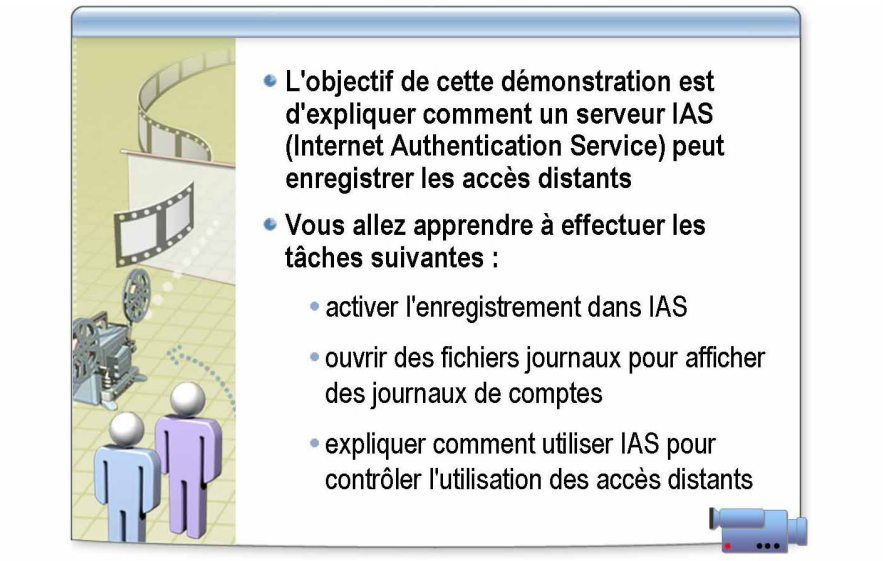
  Le verrouillage du compte d'accès à distance doit correspondre à une authentification par comptage et à un mécanisme de verrouillage qui évite une attaque par dictionnaire du mot de passe d'un utilisateur.

- La connexion doit être autorisée par la stratégie d'accès distant.

  Pour obtenir le nom de la stratégie d'accès distant qui a rejeté la tentative, vérifiez que l'enregistrement des événements IAS est actif et recherchez les événements générés par IAS dont l'ID est 2. Dans le texte du message de l'événement, recherchez le nom de la stratégie d'accès distant qui se trouve à côté du champ du nom de la stratégie.

- Si vous venez de faire passer le domaine Active Directory du mode mixte au mode natif, les serveurs IAS ne peuvent plus identifier les demandes de connexion valides. Vous devez redémarrer chaque contrôleur du domaine pour r pliquer la modification.

Démonstration : Surveillance de l'accès à distance à l'aide de l'IAS



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Cette démonstration a pour objectif d'expliquer comment un serveur IAS (Internet Authentication Service) peut enregistrer les accès distants.

Objectifs

Vous allez apprendre à :

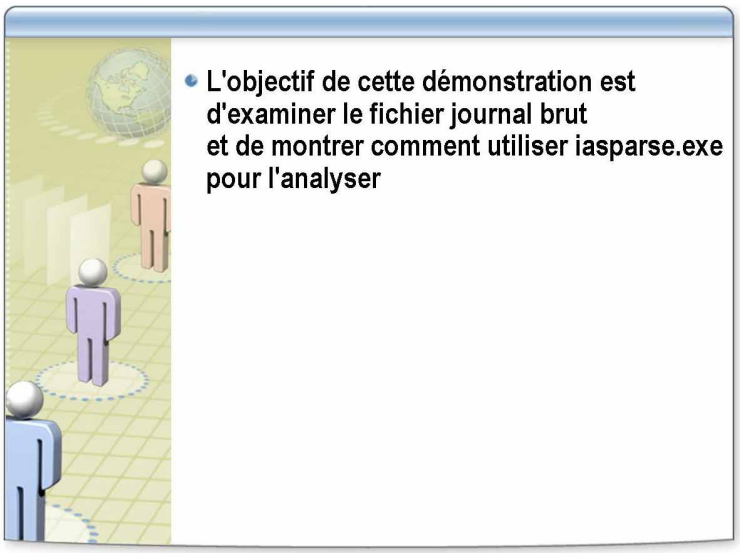
- activer l'enregistrement dans IAS ;
- ouvrir des fichiers journaux pour afficher des journaux de comptes ;
- expliquer comment utiliser IAS pour contrôler l'utilisation des accès distants.

Questions clés

Au cours de cette démonstration, vous devez vous poser les questions suivantes :

- Quels sont les options et les formats disponibles pour enregistrer les journaux IAS ?
- Pourquoi utiliser des journaux IAS ?

Démonstration : Analyse des fichiers journaux d'authentification et de gestion des comptes IAS



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Les serveurs d'accès réseau qui prennent en charge IAS peuvent enregistrer des informations d'authentification et de gestion des comptes sur les connexions d'accès réseau sur un serveur RADIUS lorsque l'authentification et la gestion des comptes RADIUS sont activées. Cet enregistrement est distinct de l'enregistrement des événements dans le journal système. Vous pouvez utiliser les informations enregistrées sur le serveur IAS pour identifier l'utilisation des accès distants et les tentatives d'authentification.

Les informations d'authentification et de gestion des comptes IAS sont enregistrées dans des fichiers journaux dans le dossier *racinesystème*\system32\LogFiles du serveur IAS.

Analyse du fichier journal brut

Pour afficher les données enregistrées dans un fichier journal IAS :

1. Accédez à C:\MOC\2189\Labfiles.
2. Double-cliquez sur in0302.log.

Notez que le format des données du fichier journal n'est pas très lisible.

Analyse du fichier à l'aide de iasparse.exe

L'utilitaire iasparse.exe des outils de support Windows Server 2003 peut analyser un fichier journal pour le rendre plus lisible.

Pour analyser le fichier journal :

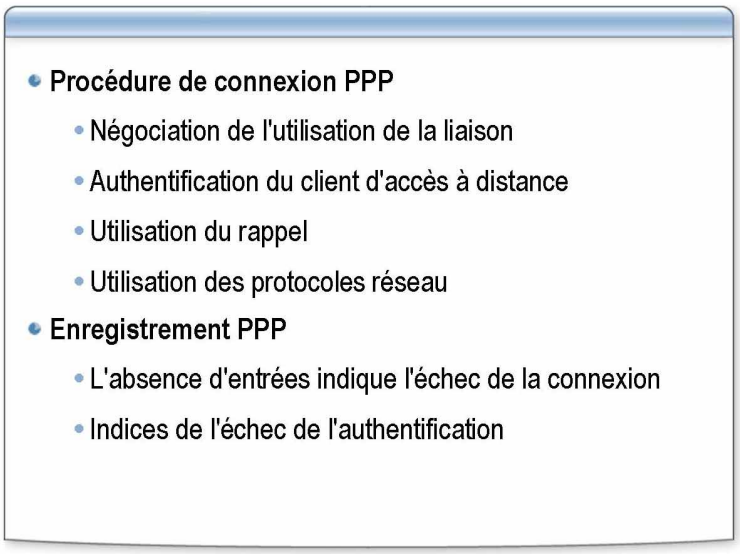
1. Ouvrez une fenêtre d'invite de commandes.
2. Accédez au répertoire C:\Program Files\Support Tools.
3. Entrez la commande **iasparse -f:C:\MOC\2189\Labfiles\in0302.log**

   Revenez au début de la sortie ; vous remarquez que l'entrée des données brutes apparaît. Les données analysées figurent sous cette entrée, chaque ligne contenant un attribut et sa valeur associée.

La sortie de l'utilitaire iasparse indique que ce fichier contient deux entrées : un accès : demande et accès rejeté. L'entrée de rejet d'accès explique le motif du refus.

Remarque Pour plus d'informations sur les attributs et les valeurs des attributs enregistrés dans ces fichiers journaux, consultez le document « Interpreting IAS Logs » dans le dossier C:\MOC\2189\labfiles\.

Enregistrement PPP



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Les journaux PPP (Point-to-Point Protocol) fournissent des informations que vous pouvez utiliser pour résoudre les problèmes de connexion des clients.

Procédure de connexion PPP

Après l'établissement d'une connexion physique ou logique à un serveur d'accès distant basé sur PPP, les négociations suivantes se produisent pour établir une connexion PPP :

- Négociation de l'utilisation de la liaison

  PPP utilise le protocole LCP (Link Control Protocol) pour négocier les paramètres de la liaison, tels que la taille de trame PPP, l'utilisation de liaisons multiples et l'utilisation d'un protocole d'authentification PPP spécifique.

- Authentification du client d'accès à distance

  Le client et le serveur échangent des messages en fonction du protocole d'authentification négocié. Si EAP est utilisé, le client et le serveur négocient une méthode EAP spécifique, appelée type EAP, puis échangent des messages de ce type.

- Utilisation du rappel

  Si le rappel est configuré pour les connexions à distance, la connexion physique prend fin et le serveur d'accès distant rappelle le client.

- Utilisation des protocoles réseau

  Cette procédure implique l'utilisation d'une série de protocoles NCP (Network Control Protocol) pour configurer les protocoles réseau qu'utilise le client d'accès à distance.

La connexion PPP résultante reste active jusqu'à ce que la liaison soit coupée pour l'une des raisons suivantes :

- L'utilisateur ou l'administrateur a déconnecté explicitement la connexion.
- La liaison a été coupée à la suite du dépassement du délai d'inactivité.
- Une erreur de communication irrécupérable s'est produite.

Enregistrement PPP

Les connexions d'accès à distance et VPN (PPTP (Point-to-Point Tunneling Protocol) et L2TP) reposent sur PPP pour établir une connexion, authentifier les utilisateurs et affecter des adresses IP aux connexions d'accès à distance. Vous pouvez activer l'enregistrement dans un fichier journal PPP pour identifier les problèmes de connexion PPP. En analysant les entrés du journal PPP, vous pouvez savoir si une connexion a échoué.

Si la session PPP n'a pas démarré, le journal PPP ne contient aucune entrée associée à la tentative de connexion. L'absence d'entrée indique que la connexion a échoué au cours ou avant l'entrée des informations de connexion textuelles.

Si le journal PPP contient des entrées, leur nature peut vous aider à identifier les éléments qui ont échoué au cours de la tentative de connexion. Lorsque toutes les autres sources d'informations ne vous permettent pas d'identifier les problèmes, les journaux PPP vous fournissent un très bon moyen de les identifier.

Activation de l'enregistrement PPP

Pour les serveurs qui exécutent Routage et accès distant, vous pouvez activer l'enregistrement PPP sous l'onglet **Enregistrement** de la page des propriétés d'un serveur d'accès distant. Pour un client d'accès à distance Windows Server 2003, utilisez Netsh pour activer l'enregistrement PPP.

Une fois l'enregistrement activé, l'ordinateur enregistre toutes les activités PPP dans le fichier ppp.log du dossier *racinesystème*\Tracing.

Important Du fait que l'enregistrement PPP utilise des ressources système et l'espace du disque dur, il est recommandé de le désactiver une fois les opérations de résolution des problèmes terminées.

Échec de l'authentification

Les journaux PPP peuvent également vous aider à identifier un problème lorsqu'il est lié à l'échec de l'authentification (problème de mot de passe ou de nom d'utilisateur). Dans ce cas, le journal doit contenir des informations similaires à celles qui figurent ci-dessous. (En supposant que LCP aboutit, l'étape suivante est l'authentification.)

- Phase d'authentification démarrée

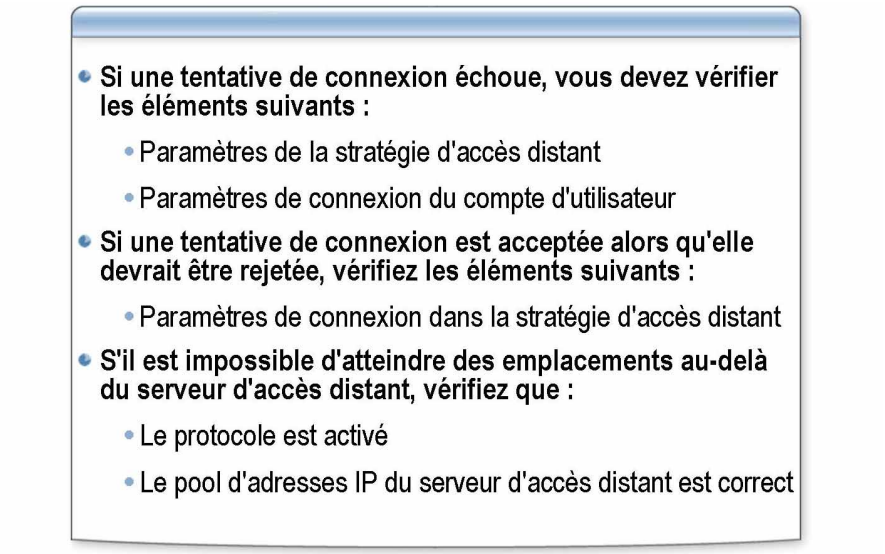
En parcourant le journal depuis ce point, vous pouvez peut-être trouver un message similaire aux messages suivants :

- Auth Protocol c023 terminated with error 4 (fin du protocole d'authentification c023 avec erreur 4)
- Auth Protocol c223 terminated with error 7 (fin du protocole d'authentification c223 avec erreur 7)

Ces messages indiquent que la négociation de l'authentification a eu lieu et que la connexion a échoué. Dans le premier cas (c023), le protocole incriminé est PAP (Password Authentication Protocol). Dans le second cas, le protocole incriminé est CHAP. Si vous recevez ces messages, procédez comme suit :

- Vérifiez votre nom d'utilisateur et votre mot de passe pour savoir s'ils sont corrects.
- Vérifiez les paramètres de l'onglet **Sécurité** de l'entrée d'annuaire téléphonique que vous utilisez. Ici, la valeur maximale du paramètre est **Accepter toute authentification (texte en clair inclus)**, car ce paramètre signifie qu'une connexion peut avoir lieu si le fournisseur de service Internet demande PAP ou CHAP.
- La boîte de dialogue **Se connecter à** contient le champ DOMAINE. Si vous ne vous connectez pas à un serveur Microsoft Windows NT® Server qui exécute RAS (Remote Access Service), vérifiez que cette case à cocher est inactive car, dans le cas contraire, elle peut parfois provoquer l'échec du protocole CHAP.
- Si l'authentification n'aboutit toujours pas, vérifiez le nom d'utilisateur et le mot de passe auprès de votre fournisseur de service Internet ou du service technique de votre entreprise. Vous devez les contacter pour identifier l'origine de l'échec de la connexion.

Connexions d'accès à distance



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Plusieurs composants de résolution des problèmes s'appliquent à tous les types de connexions d'accès à distance. En outre, il existe des symptômes, des outils et des procédures pour chaque problème de connexion, qui peuvent vous aider à trouver la solution.

Échec des tentatives de connexion

Si une tentative de connexion est rejetée alors qu'elle devrait être acceptée, vérifiez que :

- le service d'accès distant est actif ;
- les ports PPTP et L2TP sont actifs ;
- la stratégie d'accès distant est configurée pour utiliser une méthode d'authentification commune ;
- le serveur est configuré pour utiliser une méthode d'authentification commune ;
- les paramètres de la stratégie d'accès distant et les conditions coïncident ;
- les paramètres du compte d'utilisateur sont corrects ;
- la configuration du fournisseur d'authentification est correcte ;
- le serveur VPN a été joint au domaine s'il s'agit d'un serveur VPN membre d'un domaine Windows en mode natif ;
- l'ordinateur du serveur VPN peut dialoguer avec le serveur RADIUS pour l'authentification IAS.

Tentative acceptée qui devrait être rejetée

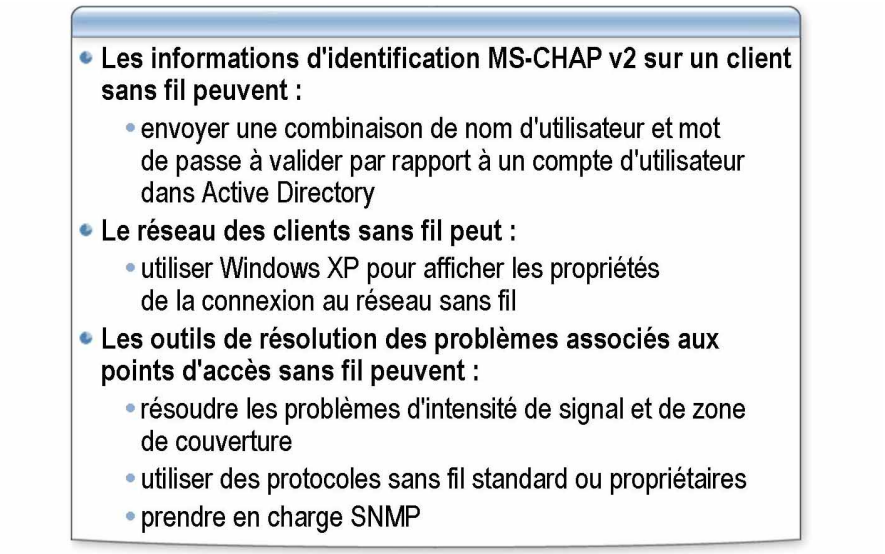
Si une tentative de connexion est acceptée alors qu'elle devrait être rejetée, vous devez vérifier que les paramètres de la connexion n'obtiennent pas l'autorisation via les stratégies d'accès à distance.

Impossibilité de communiquer avec le serveur VPN

Si le client ne parvient pas à atteindre des emplacements au-delà du serveur VPN, vérifiez que :

- le protocole peut effectuer le routage ;
- les pools d'adresses IP du serveur d'accès distant sont corrects ;
- les routeurs se trouvent de chaque côté de la connexion VPN (pour les connexions entre routeurs).

Authentification des accès sans fil



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Si vous utilisez IAS pour l'authentification RADIUS des clients sans fil, la méthode la plus sûre et recommandée, vous devez vérifier que le serveur IAS est configuré et qu'il fonctionne correctement. Vous devez également vérifier le certificat du client et celui du serveur selon la méthode EAP que vous décidez d'implémenter. Si vous choisissez EAP-TLS, vous avez besoin des deux certificats. Si vous utilisez Protected EAP (PEAP)/MS-CHAP v2, vous n'avez besoin que du certificat du serveur RADIUS.

Si vous utilisez l'authentification EAP-TLS, vous devez vérifier que le certificat du serveur d'authentification et celui du client sont valides.

Informations d'identification MS-CHAP v2 des clients sans fil

Un client sans fil qui utilise PEAP/MS-CHAP v2 envoie un nom d'utilisateur et un mot de passe à valider par rapport à un compte d'utilisateur dans Active Directory, au lieu d'utiliser un certificat pour authentifier un utilisateur. Pour que la validation de compte aboutisse, vous devez vérifier les points suivants :

- Le partie domaine du nom d'utilisateur doit correspondre au domaine du serveur IAS ou à un domaine qui a une approbation bidirectionnelle avec le domaine du serveur IAS.
- La partie nom de compte du nom de l'utilisateur doit correspondre à un compte valide dans le domaine.
- Le mot de passe du compte doit être correct.

Pour vérifier les informations d'identification, demandez aux utilisateurs des clients sans fil de se connecter à leur domaine en utilisant un ordinateur déjà connecté au réseau en utilisant par exemple une connexion Ethernet (si possible).

Informations réseau des clients sans fil

Si le système d'exploitation d'un client sans fil est Microsoft Windows XP, vous pouvez utiliser la page Connexions réseau pour afficher les propriétés de la connexion sans fil. Cette page contient l'onglet **Configuration réseaux sans fil** qui affiche les réseaux sans fil disponibles et favoris. Vous pouvez définir les propriétés d'association et d'authentification de la page Propriétés d'un réseau sans fil.

Pour plus d'informations sur les opérations générales de résolution des problèmes associés aux clients sans fil Windows XP, consultez l'article 313242 « How to Troubleshoot Wireless Network Connections in Windows XP » (en anglais), à l'adresse http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B313242 dans la Base de connaissances de Microsoft.

Outils de résolution des problèmes associés aux points d'accès sans fil

Les outils de résolution des problèmes d'un point d'accès sans fil dépendent du groupe d'outils et du logiciel d'administration fournis avec le point d'accès sans fil. Par exemple :

- Certains points d'accès sans fil fournissent des outils d'analyse de la force du signal que vous pouvez utiliser pour résoudre un problème de signal faible et de couverture.
- Un point d'accès sans fil peut également fournir un utilitaire PING pour vérifier l'accès au point d'accès en utilisant des protocoles standard ou des protocoles sans fil propriétaires.
- Un point d'accès sans fil peut également prendre en charge le protocole SNMP (Simple Network Management Protocol) et la base MIB 802.11 (Management Information Base).

Clés WEP

Lorsque vous activez WEP (Wired Equivalent Privacy), vous spécifiez qu'une clé réseau doit être utilisée pour le cryptage. Une clé réseau peut vous être fournie automatiquement (elle peut être fournie, par exemple, dans votre carte réseau sans fil) ou vous pouvez la définir en la configurant vous-même. Si vous la configurez vous-même, vous devez utiliser la longueur de clé et le nombre de clés corrects (vous pouvez en configurer quatre) et entrer correctement la clé. Si vous ne configurez pas correctement la clé, vous ne pouvez pas vous connecter au réseau. Pour configurer correctement la clé, contactez l'administrateur du réseau.

Pour plus d'informations sur les outils et les techniques de résolution des problèmes des points d'accès sans fil, consultez la documentation des points d'accès sans fil.

Problèmes VPN courants

Problème	Stratégie de résolution
Délai de connexion TCP	Vérifier le port 1723
Filtrage des paquets	Vérifier que les paquets ne sont pas bloqués
Client Winsock Proxy	Vérifier qu'aucun client proxy n'est activé
Protocole de tunnel	Vérifier que le serveur prend en charge le protocole
Certificats	Vérifier que les certificats de l'ordinateur sont installés sur le serveur VPN
Connexions PPTP	Vérifier la longueur du mot de passe utilisateur
NAT-T	Vérifier que le client prend en charge IPSec NAT Traversal (NAT-T)

**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Pour résoudre les problèmes de connexion VPN, vous devez résoudre les problèmes de connexion IP, d'accès à distance et à la demande, de routage et IPSec.

Problèmes VPN courants

La plupart des problèmes VPN sont liés aux tunnels. La liste suivante vous fournit un point de départ pour effectuer la procédure de résolution des problèmes :

- Vérifiez vos messages d'erreur.

  Si vous avez reçu l'erreur 678 pour une connexion PPTP, cela implique que le serveur VPN ne répond pas à la suite du dépassement du délai d'attente dans la connexion TCP au serveur VPN. Cette erreur se produit si le port TCP 1723 est bloqué entre le client VPN et le serveur VPN.

- Vérifiez que le filtrage des paquets sur une interface de routeur entre le client VPN et le serveur VPN n'empêche pas l'envoi du trafic du protocole de tunnel.

  Sur un serveur VPN basé sur Windows Server 2003, le filtrage des paquets IP peut être configuré dans les propriétés avancées TCP/IP et dans le composant logiciel enfichable Routage et accès distant. Vérifiez ces deux éléments pour identifier les filtres qui pourraient exclure le trafic de la connexion VPN.

- Vérifiez que le client Winsock Proxy n'est pas actif sur le client VPN.

  Lorsque le client Winsock Proxy est actif, les appels de l'API (Application Programming Interface), tels que ceux utilisés pour créer les tunnels et envoyer les données dans le tunnel, sont interceptés et envoyés à un serveur proxy configuré.

- Vérifiez que le protocole de tunnel du client VPN est pris en charge par le serveur VPN.

  Par défaut, l'option de type de serveur **Automatique** est active sur les clients VPN d'accès à distance Windows Server 2003, ce qui implique qu'ils tentent d'établir une connexion VPN basée sur L2TP sur IPSec, puis d'établir une connexion VPN basée sur PPTP.

- Si l'option de type de serveur **PPTP (Point-to-Point Tunneling Protocol)** ou **L2TP (Layer-2 Tunneling Protocol)** est active, vérifiez que le protocole de tunnel est pris en charge par le serveur VPN.

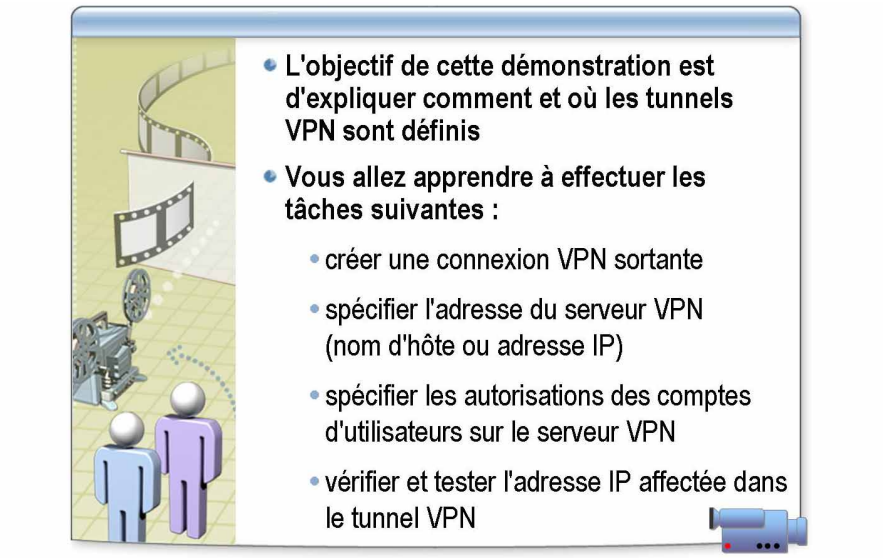
- Pour les connexions d'accès à distance L2TP sur IPSec, vérifiez que les certificats d'ordinateurs (appelés également certificats de machines) sont installés sur le client VPN et sur le serveur VPN.

- Pour les connexions PPTP qui utilisent MS-CHAP Version 1 et qui tentent de négocier le cryptage MPPE (Microsoft Point-to-Point Encryption) 40 bits, vérifiez que la longueur du mot de passe de l'utilisateur ne dépasse pas 14 caractères.

- Pour les clients L2TP/IPSec derrière un traducteur d'adresses réseau, vérifiez que le client prend en charge IPSec NAT-T (Network Address Translation Traversal).

  IPSec NAT–T est pris en charge par le client VPN Microsoft L2TP/IPSec (Windows 98, Windows Millennium Edition et Windows NT 4.0 Workstation) et par Windows Server 2003. La prise en charge de IPSec NAT–T pour les clients Windows 2000 et Windows XP est fournie avec Windows Server 2003.

Démonstration : Tester une connexion sortante



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

L'objectif de cette démonstration vise à expliquer comment et où les tunnels VPN sont définis.

Objectifs

Vous allez apprendre à :

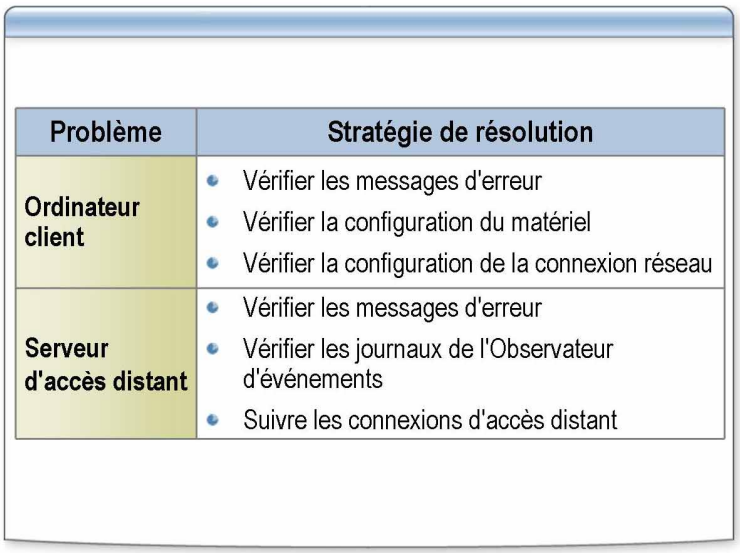
- créer une connexion VPN sortante ;
- spécifier l'adresse du serveur VPN (nom d'hôte ou adresse IP) ;
- spécifier les autorisations des comptes d'utilisateurs sur le serveur VPN ;
- vérifier et tester l'adresse IP affectée dans le tunnel VPN.

Questions clés

Au cours de cette démonstration, vous devez vous poser les questions suivantes :

- Lors de la création d'une connexion par tunnel, comment le serveur VPN est-il identifié ?
- Comment mettre cette connexion à la disposition de tous les utilisateurs de l'ordinateur ?
- Comment déterminer la durée d'une connexion ?

Procédure de résolution des problèmes d'accès à distance au réseau



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Les opérations de résolution des problèmes d'accès à distance au réseau impliquent d'exécuter un certain nombre d'opérations de résolution de problèmes sur les modems utilisés pour établir les connexions. Toutefois, il se peut que vous deviez également résoudre des problèmes associés aux clients, car en règle générale, ces derniers sont à l'origine de la plupart des problèmes.

Procédure de résolution des problèmes sur les ordinateurs clients

La majorité des opérations de résolution des problèmes de configuration du serveur d'accès distant portent sur l'ordinateur client et impliquent les étapes suivantes :

1. Notez les messages d'erreur que vous recevez, puis consultez les journaux de l'Observateur d'événements.

   Le journal système, en particulier, peut fournir des informations utiles pour résoudre les problèmes.

2. Vérifiez la configuration du matériel.
3. Après avoir vérifié que le matériel fonctionne correctement, vérifiez que la configuration de la connexion réseau est adaptée au type de serveur appelé. Vérifiez particulièrement les paramètres de sécurité.

Vous constaterez que le problème provient bien souvent de la modification par l'utilisateur de sa configuration. Si vous assistez un utilisateur, veillez à lui poser les questions pertinentes pour déterminer la modification qu'il a effectuée.

Recréer l'entrée de connexion réseau peut vous aider à déterminer rapidement si le problème provient d'une erreur de configuration sur l'ordinateur client. Si la nouvelle connexion permet d'accéder au serveur d'accès distant, cela implique que la connexion réseau d'origine était mal configurée.

Procédure de résolution des problèmes sur les serveurs distants

Bien que les problèmes d'accès distant se produisent moins fréquemment sur le serveur, vous trouverez des outils de dépannage plus performants sur le serveur plutôt que sur le client. Les instructions suivantes de résolution des problèmes sont similaires pour le serveur et le client :

1. Notez toujours les messages d'erreur que vous recevez, car ils facilitent les opérations de résolution des problèmes.
2. Dans l'Observateur d'événements, recherchez les événements qui peuvent indiquer les erreurs qui se sont produites lorsque le client a appelé le serveur.
3. Retracez les connexions d'accès à distance.

Si le fichier journal contient des erreurs, il se peut que vous deviez remplacer le modem par un modem pris en charge par Windows (n'importe quel modem compatible Hayes convient).

Autres problèmes d'accès à distance

Vous pouvez être également confronté à d'autres problèmes d'accès à distance. En voici quelques-uns :

- Communication entre l'ordinateur et le modem

  L'impossibilité pour un ordinateur de dialoguer avec un modem est bien souvent à l'origine des problèmes du serveur d'accès distant, notamment si le serveur utilisait le service d'accès distant avant une mise à jour matérielle. Vous devez vérifier la connexion entre l'ordinateur et le modem en vous assurant que le port série fonctionne correctement.

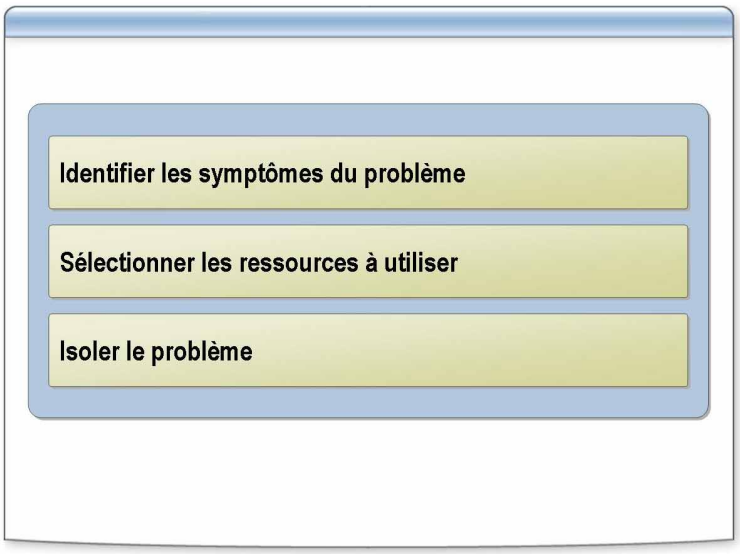
- Communication modem à modem

  Après avoir déterminé que vous pouvez communiquer avec le modem, utilisez HyperTerminal pour vérifier que vous pouvez établir des connexions avec un autre modem.

- Communications entre le service d'accès distant et le modem

  Après avoir vérifié que le modem peut se connecter à l'ordinateur client et autres modems, vous devez vérifier que Routage et accès distant peut utiliser correctement le modem. Pour vérifier le flux de configuration des communications entre Routage et accès distant et le modem, vous devez ajouter le journal à l'onglet **Diagnostics** des propriétés du modem.

Instructions de résolution des problèmes d'accès à distance



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

La résolution des problèmes d'accès à distance englobe la procédure et les outils qui permettent d'identifier les problèmes et de les résoudre. Suivez les instructions ci-dessous pour définir votre stratégie de résolution des problèmes.

- Identifiez les symptômes du problème

  En premier lieu, vous devez identifier les symptômes du problème. Vous devez également vérifier les ressources du réseau pour vous assurer qu'il ne s'agit pas d'un problème matériel. Les symptômes que vous identifiez doivent vous permettre de déterminer si le client ou le serveur est à l'origine du problème.

- Sélectionnez les ressources à utiliser

  Sélectionnez les ressources appropriées en fonction des symptômes du problème. Une fois les ressources sélectionnées, vous devez activer l'audit des événements de connexion et l'audit des événements de connexion aux comptes.

- Isolez le problème

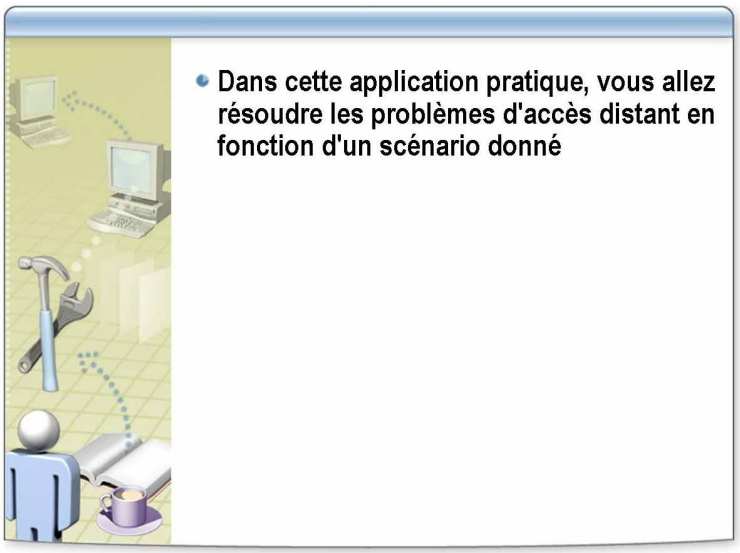
  Maintenant, vous allez utiliser les ressources sélectionnées pour isoler le problème. Si le problème provient du client, vérifiez ses paramètres de configuration, tels que :

  - numéro de téléphone ;
  - nom d'utilisateur et mot de passe ;
  - périphérique de connexion ;
  - cryptage ;
  - protocoles d'authentification ;
  - type VPN ;
  - pilotes et services utilisés avec la connexion.

Si le problème provient du serveur :

- vérifier les propriétés de numérotation de l'utilisateur ;
- vérifier les journaux et les événements ;
- vérifier les stratégies d'accès à distance ;
- vérifier la connectivité du serveur (connexion d'appel entrant ou LAN) ;
- vérifier si Routage et accès distant est actif ;
- rechercher les connexions entrantes ;
- rechercher les ports disponibles ;
- rechercher les adresses disponibles ;
- vérifier qu'il existe un fournisseur d'authentification approprié et qu'il est correctement configuré.

Application pratique : Résolution des problèmes d'authentification des accès à distance



**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Introduction

Dans cette application pratique, vous allez identifier les étapes de résolution d'un problème d'accès à distance.

Objectif

L'objectif de cette application pratique vise à résoudre un problème d'accès à distance.

Instructions

1. Lisez le scénario.
2. Préparez-vous à discuter des difficultés associées à cette tâche après l'application pratique.

Scénario

Contoso, Ltd vient de mettre à jour tous ses serveurs Windows en installant Windows Server 2003. De plus, la société impose aux utilisateurs distants d'utiliser L2TP pour se connecter au réseau de l'entreprise. La société a implémenté une infrastructure de certificats pour émettre des certificats d'utilisateurs et des certificats d'ordinateurs et a fourni aux utilisateurs distants des cartes à puce, des lecteurs de cartes à puce et les instructions d'installation associées qui ont été validées.

Avant la mise à jour, tous les utilisateurs distants se connectaient sans problème au réseau de l'entreprise en utilisant PPTP. Depuis l'implémentation des connexions L2TP, certains utilisateurs distants ne parviennent plus à se connecter.

Les ordinateurs de tous les clients distants utilisent Windows XP Professionnel.

Application pratique

Comment résolvez-vous ce problème ?

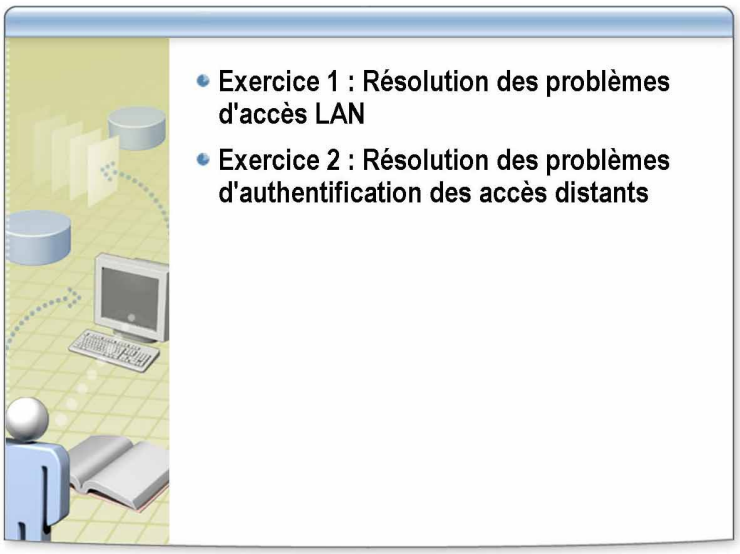
Vérifiez les points communs aux utilisateurs qui ne parviennent pas à se connecter. De même, vérifiez les points communs aux utilisateurs qui peuvent se connecter.

Du fait que vous savez que certains utilisateurs parviennent à se connecter, il est peu probable que le serveur soit à l'origine du problème. Vous pouvez toujours vérifier le journal système du serveur qui exécute Routage et accès distant pour y rechercher des erreurs ou des avertissements, mais il est préférable de vous concentrer sur le client.

Recherchez des informations pertinentes dans le journal système du client. S'il existe des problèmes de certificat, les informations associées figurent dans les journaux. Vous pouvez ensuite exécuter les opérations de résolution qui correspondent à l'erreur détectée.

Vérifiez si les utilisateurs qui ne parviennent pas à se connecter utilisent un NAT. Si tel est le cas, vérifiez si leur système d'exploitation Windows XP a été mis à jour avec le logiciel de mise à jour NAT-T. Sans cette mise à jour, les utilisateurs ne peuvent pas utiliser L2TP/IPSec via un NAT. Cette mise à jour peut expliquer la raison pour laquelle certains utilisateurs peuvent se connecter (peut-être ceux qui utilisent une connexion à distance pour se connecter à leur fournisseur de service Internet) et d'autres pas.

Atelier A : Résolution des problèmes d'accès réseau



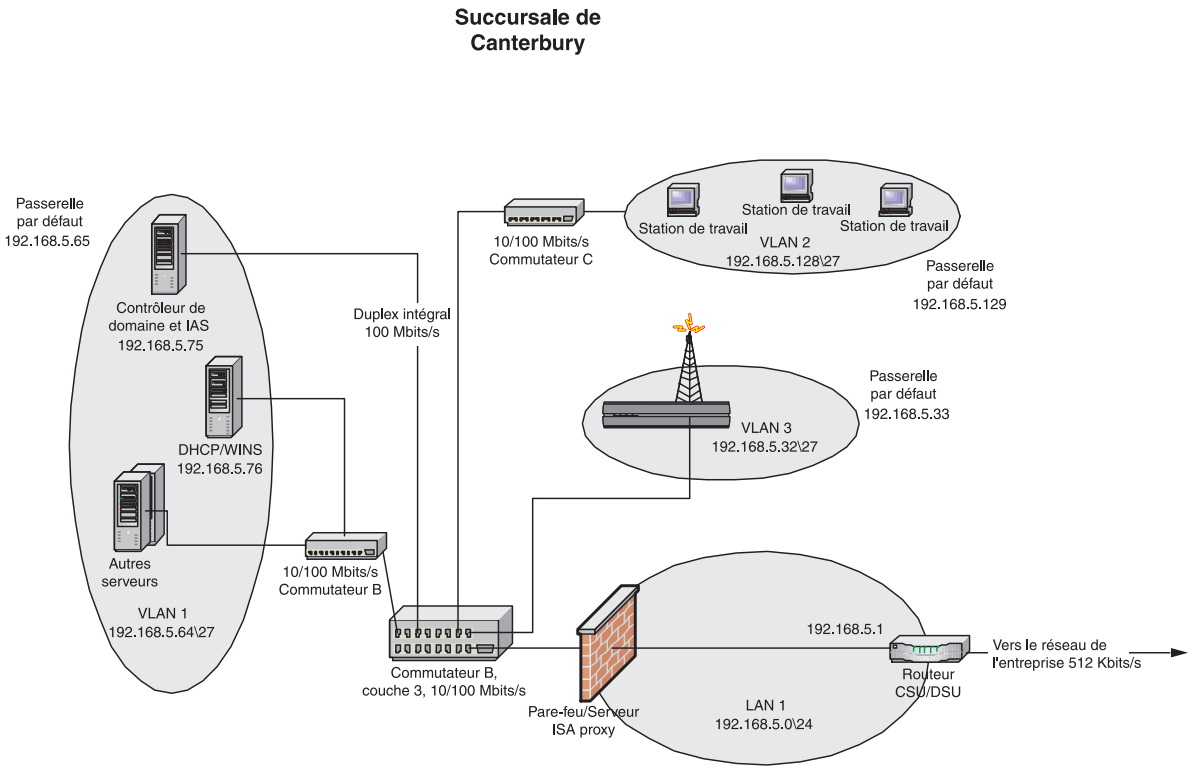
**********DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR**********

Objectifs

À la fin de cet atelier, vous serez à même de résoudre les problèmes de connectivité réseau et d'authentification en utilisant les informations collectées.

Scénario

Vous êtes ingénieur système chez Northwind Traders et on vous demande d'aider un nouveau service d'assistance en ligne MCSA (Microsoft Certified Systems Administrator) à résoudre les problèmes de connexion réseau et d'authentification de la filiale Canterbury au Royaume-Uni. Les stations de travail et les serveurs se trouvent dans Northwind Traders Active Directory et exécutent Windows XP Professionel ou Windows Server 2003. Certains problèmes sont liés aux utilisateurs d'ordinateurs de bureau du LAN de la société, mais il existe également d'autres problèmes liés aux utilisateurs distants qui se connectent au réseau en utilisant des connexions VPN.



Durée approximative de cet atelier : 30 minutes

Exercice 1
Résolution des problèmes d'accès LAN

Dans cet exercice, vous aller résoudre un problème auquel est confrontée la filiale Canterbury de Northwind Traders. Vous vous trouvez dans le bureau de Londres et vous devez obtenir des informations pour résoudre le problème à distance.

Scénario

Un utilisateur de la filiale de Canterbury ne parvient pas parfois à accéder aux ressources lorsqu'il se connecte au réseau via le LAN. On vous demande de résoudre le problème en vous fournissant les informations suivantes :

- L'ordinateur portable de l'utilisateur est connecté au VLAN 192.168.5.128/27.
- L'ordinateur portable démarre correctement et affiche un écran d'ouverture de session de domaine.
- Lorsque l'utilisateur se connecte en utilisant les informations d'identification de domaine, il ne parvient parfois qu'à se connecter aux ressources de son propre ordinateur.
- Lorsqu'il parvient à se connecter, il est parfois confronté à des erreurs intermittentes d'applications, telles que Microsoft Internet Explorer, qui signalent des erreurs telles que “Serveur DNS introuvable” ou qui tardent à charger une page Web.
- L'utilisateur signale qu'il n'est pas parvenu récemment à utiliser son ordinateur pendant plus de deux heures sans problèmes.
- Il indique que s'il se déconnecte du réseau et utilise un accès sans fil, aucune erreur ne se produit. Toutefois, l'accès sans fil est trop lent pour les applications multimédias qu'il utilise.

Tâches	Instructions spécifiques
1. Documenter la procédure à utiliser pour résoudre ce problème.	
2. Analyser les données capturées.	**a.** Les données sont stockées dans : C:\MOC\2189\labfiles\lab11.exe. **b.** Les fichiers ont été compressés et doivent être décompressés pour effectuer l'atelier. Chaque fichier contient des informations sur les données capturées suivies des résultats. **c.** Dans C:\MOC\2189\labfiles, créez le dossier **analysis**. **d.** Copiez lab11.exe vers le dossier. **e.** Exécutez lab11.exe pour décompresser les fichiers dans le dossier analysis.
3. Identifier l'origine probable du problème.	

Exercice 2
Résolution des problèmes d'authentification des accès distants

Dans cet exercice, vous allez expliquer comment vous recherchez les problèmes éventuels associés aux serveurs d'accès distant VPN qui doivent être déployés dans le centre de données de Londres.

Scénario

Le personnel de l'assistance technique en ligne devra répondre aux appels de demande d'assistance de la première ligne et il se peut que vous deviez résoudre les problèmes de la seconde ligne. Vous devez documenter les journaux qui doivent être contrôlés et capturés au cours des premières étapes du déploiement. La période initiale de résolution des problèmes est inférieure à deux semaines. On vous fournit les informations suivantes :

- Les trois serveurs VPN à déployer dans le centre de données de Londres prendront en charge entre 30 et 50 connexions simultanément.
- Les trois serveurs ont été testés dans une configuration pilote et leurs performances et leur fonctionnalité ont été validées.
- Les serveurs VPN sont configurés avec deux entrées de serveur IAS pour les opérations d'authentification RADIUS.
- Le logiciel serveur IAS est installé sur deux contrôleurs de domaine du centre de données de Londres.
- Des cartes à puce ont été fournies aux employés autorisés à utiliser les serveurs VPN.
- Connection Manager a été déployé sur les ordinateurs des utilisateurs et les informations de configuration ont été validées sur le pilote.
- Les certificats des ordinateurs clients ont été déjà déployés en utilisant Services de certificats.
- Les seules connexions VPN autorisées utilisent L2TP/IPSec.

Tâches	Instructions spécifiques
1. Documenter la méthodologie de résolution des problèmes, les outils, les journaux et les journaux de l'Observateur d'événements considérés essentiels pour résoudre les problèmes de déploiement qui peuvent se produire.	